Supreme Court, U.S.
FILED
(1)
00 967 DEC 1 3 2000

No.

IN THE
Supreme Court of the United States

STEVEN D.C. BIGELOW, *Petitioner,*

v.

DEPARTMENT OF DEFENSE, *Respondent.*

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

PETITION FOR WRIT OF CERTIORARI

EUGENE R. FIDELL
(Counsel of Record)
DAVID P. SHELDON
JAMES L. FELDESMAN
FELDESMAN, TUCKER, LEIFER,
FIDELL & BANK LLP
2001 L Street, N.W.
Washington, D.C. 20036
(202) 466-8960

Attorneys for Petitioner

DECEMBER 2000

128 PP

QUESTIONS PRESENTED

1. Is an otherwise unauthorized release of Privacy Act information permissible without specific evidence that the releasing official determined that the recipient had a "need to know" on the theory that, under the Defense Department's Personnel Security Program regulation, supervisors have a *per se* need to know the entire contents of their supervisees' security files?

2. In light of *Bowen v. Georgetown University Hospital*, 488 U.S. 204 (1988), is an interpretation of a Defense Department regulation entitled to deference when it is advanced only by Assistant United States Attorneys and junior agency "of counsel," rather than any policy-level agency official?

TABLE OF CONTENTS

Page

OPINIONS BELOW 2

JURISDICTION 2

GOVERNING STATUTE AND REGULATIONS . . 2

STATEMENT 3

1. Summary 3
2. Regulatory Framework 4
3. Lt Col Bigelow's DD Form 398 5
4. Privacy Act Violation 5
5. Proceedings in the District Court 6
6. The Decision of the Court of Appeals 7

REASONS FOR GRANTING THE PETITION . . . 10

I. The decision below dramatically expands the class of persons who may access others' security files and makes a hash of the Defense Department's Personnel Security Program regulation 10

II. The decision below conflicts with *Bowen* because it defers to an interpretation that has never been announced or embraced by any policy-level official 21

Conclusion 23

APPENDIX

Decision of the Court of Appeals (July 14, 2000) . . 1a
Judgment of the Court of Appeals (July 14, 2000) 15a
Order denying rehearing (Oct. 13, 2000) 17a
Order denying rehearing *En Banc* (Oct. 13, 2000) 18a
Order amending Judge Tatel's dissent from denial of rehearing and rehearing *en banc* (Oct. 25, 2000) 20a
Statement of Judge Tatel dissenting from denial of rehearing and rehearing *en banc* (corrected version) 22a
Judgment of the District Court (June 11, 1999) . 24a
Order (June 11, 1999) 25a
Transcript of proceedings in the District Court (June 11, 1999) 26a
Privacy Act of 1974, 5 U.S.C. § 552a (1994) (excerpts) 40a
Dep't of Defense Personnel Security Program, 32 C.F.R. Pt. 154 (2000) (excerpts) 58a
§ 152.2 . . . . . 58a
§ 154.3 . . . . . 58a
§ 154.9 . . . . . 65a
§ 154.47 . . . . . 69a
§ 154.55 . . . . . 70a
§ 154.56 . . . . . 75a
§ 154.60 . . . . . 77a
§ 154.65 . . . . . 81a
§ 154.66 . . . . . 82a
§ 154.67 . . . . . 82a
§ 154.68 . . . . . 83a
§ 154.69 . . . . . 84a
Dep't of Defense Privacy Program, 32 C.F.R. Pt. 310 (2000) (excerpt) 86a
§ 310.41(a) 86a

Letter from Edmund F. McBride, Chief, Information Management Division, Secretariat, Joint Staff (Aug. 19, 1997) 87a
Declaration of Col Nathan W. Noyes (June 11, 1998) 89a
Affidavit of Steven D.C. Bigelow in Support of Plaintiff's Motion to Conduct Limited Discovery (July 24, 1998) 91a

TABLE OF CITED AUTHORITIES

Page

Auer v. Robbins, 516 U.S. 1109 (1996) (mem.) . . . 22
Auer v. Robbins, 519 U.S. 452 (1997) 7, 8, 9, 22
Bigelow v. Dep't of Defense, 217 F.3d 875 (D.C. Cir. 2000) . . . . . *passim*
Bowen v. Georgetown University Hospital, 488 U.S. 204 (1988) 8, 21, 22
Britt v. Naval Investigative Service, 886 F.2d 544 (3d Cir. 1989) 13
Buffalo Crushed Stone, Inc. v. Surface Transp. Bd., 194 F.3d 125 (D.C. Cir. 1999) 8
Christensen v. Harris County, 120 S. Ct. 1655 (2000) 16
Geier v. American Honda Motor Co., Inc., 120 S. Ct. 1913 (2000) 8, 22, 23
Hernandez v. Alexander, 671 F.2d 402 (10th Cir. 1982) 14
Kargman v. Sullivan, 552 F.2d 2 (1st Cir. 1977) . . 20
Martin v. OSHRC, 499 U.S. 144 (1991) 21
Meehan v. Macy, 392 F.2d 822 (D.C. Cir. 1967), *modified*, 425 F.2d 469 (1968), *reinstated in part*, 425 F.2d 472 (1969) (en banc) (per curiam), . . . 20
O'Melveny & Myers v. F.D.I.C., 512 U.S. 79 (1994) 16
Pippinger v. Rubin, 129 F.3d 519 (10th Cir. 1997) 14
Tampa Phosphate R.R. v. Seaboard Coast Line R.R., 418 F.2d 387 (5th Cir. 1969), *cert. denied*, 397 U.S. 910 (1970) 20

Statutes:

Freedom of Information Act, 5 U.S.C. § 552 (1994) . 4
Privacy Act of 1974, 5 U.S.C. § 552a (1994) . . *passim*
5 U.S.C. § 552a(b)(1) 2, 4
10 U.S.C. § 155(a) (1994) 3
10 U.S.C. § 155(a)(3) (1994) 3
10 U.S.C. § 155(f)(2) (1994) 3
28 U.S.C. § 1254(1) (1994) 2
28 U.S.C. § 1331 (1994) 6

Regulations:

Dep't of Defense Personnel Security Program,
32 C.F.R. Pt. 154 (2000) . . . . . *passim*
§ 154.2(b) 11
§ 154.3(q) 15
§ 154.7(a) 17
§ 154.9(a) 14, 16
§ 154.9(c)(3) 14, 16
§ 154.9(c)4) 16
§ 154.19 15
§ 154.55(b)(1) 17, 18
§ 154.60 . . . . . 8, 9
§ 154.60(a) 17
§ 154.60(c)(1) 15
§ 154.65 . . . . . 4, 5
§ 154.66 5
§ 154.67 4
§ 154.69(a) 5
App. A 15
App. H 17
32 C.F.R. Pt. 155 (2000) 11
Dep't of Defense Privacy Program,
32 C.F.R. Pt. 310 (2000) 3
§ 310.41(a) 4

Miscellaneous:

Brief for the United States as Amicus Curiae, *Auer v. Robbins*, 1995 U.S. Briefs 897 [LEXIS], No. 95-897 22
Brief for the United States as Amicus Curiae Supporting Affirmance, *Geier v. American Honda Motor Co., Inc.*, No. 98-1811, <www.usdoj.gov/osg/briefs/1999/3mer/1ami/98-1811/mer.ami.html> 23
Dep't of Defense, *Defense Almanac* (1999), <www.defenselink.mil/pubs/almanac/> 11
Defense Security Service, *Personnel Security Investigations, Frequently Asked Questions*, <www.dss.mil/aboutdss/faq.htm> 4
Fed. R. Civ. P. 56(f) 7
GAO, *Audit Report, Security Clearance Investigative Priorities*, Rep. No. D-2000-11 (Apr. 5, 2000) 12
GAO, National Security and International Affairs Div., *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks* (Letter Report, Oct. 27, 1999, GAO/NSIAD-00-12) 12
John F. Joyce, *The Privacy Act: A Sword and a Shield But Sometimes Neither*, 99 MIL. L. REV. 113 (1983) 20
Edward T. Pound, *Security Clearance Backup Continues*, USA Today, Aug. 25, 2000, at 8A . . . 12

TABLE OF PARALLEL PROVISIONS
Dep't of Defense Personnel Security Program

Internal DOD Version	32 C.F.R. Pt. 154
¶ 2-101	§ 154.6(b)
¶ 2-200	§ 154.7
¶ 2-306(c)	§ 154.8(g)
¶ 2-402(c)	§ 154.9(c)(3)
¶ 6-100	§ 154.40
¶ 8-102	§ 154.55(c)
¶ 9-100	§ 154.60(a)
¶ 9-102	§ 154.60(c)
¶ 9-104	§ 154.60(e)
¶ 10-100	§ 154.65
¶ 10-102	§ 154.67
¶ 10-103	§ 154.68
¶ 10-104	§ 154.69

IN THE

Supreme Court of the United States

STEVEN D.C. BIGELOW, *Petitioner,*

v.

DEPARTMENT OF DEFENSE, *Respondent.*

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

PETITION FOR WRIT OF CERTIORARI

Lieutenant Colonel Steven D.C. Bigelow, U.S. Air Force (Retired), respectfully prays that a writ of certiorari issue to review the judgment below.

The case raises the important question whether, under the Privacy Act and the Defense Department's Personnel Security Program regulation, a supervisor has a *per se* "need to know" the contents of his or her supervisees' security files and whether "need to know" is to be determined by the individual seeking access to protected records or by the officials responsible for maintaining and safeguarding those records. Left undisturbed, the decision below will grant to literally tens of thousands of military and civilian supervisors a license to rummage. It creates a gaping hole in those important parts of DOD's regulation which, consistent with the Privacy Act, purport to impose strict limits on the accessibility of sensitive personnel information.

The case also raises the important and recurring generic issue of whether an interpretation of an agency regulation is entitled to deference even if no policy-level official has ever announced or embraced that interpretation.

Opinions Below

The decision of the Court of Appeals is reported at 217 F.3d 875 and is reproduced in the Appendix ("Pet. App.") at 1a. The unpublished orders denying rehearing and rehearing *en banc* appear at Pet. App. 17a and 18a. The order amending Judge Tatel's dissent from the denial of rehearing and rehearing *en banc* appears at Pet. App. 20a, and the dissent (as corrected) appears at Pet. App. 22a. The transcript of proceedings in and the judgment of the District Court (Jackson, *J.*) appear at 26a and 25a.

Jurisdiction

The Court of Appeals decided the case on July 14, 2000, and denied rehearing and rehearing *en banc* on October 13, 2000. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

Governing Statute and Regulations

The governing statute is the Privacy Act of 1974. 5 U.S.C. § 552a. Of particular relevance is the exception that permits disclosure of otherwise nondisclosable records "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." *Id.* § 552a(b)-(1). The governing regulations are DOD's Personnel

Security Program regulation, 32 C.F.R. Pt. 154 (2000),[1] and Privacy Program regulation, 32 C.F.R. Pt. 310 (2000). Pertinent portions of the statute and regulations are reproduced in the Appendix.

Statement

1. *Summary.* The Joint Staff assists the Joint Chiefs of Staff. 10 U.S.C. § 155(a). Only those who are "considered to be the most outstanding" are selected to serve on the Joint Staff, *id.* § 155(a)(3), a prestigious, career-enhancing assignment. *See id.* § 155(f)(2). Lt Col Bigelow (then a Major) was an Air Force officer assigned to the Joint Staff's Information Warfare and Special Technical Operations Center. His supervisor, Army Colonel Nathan W. Noyes, was able to obtain access to Lt Col Bigelow's security file, which contained adverse information. Col Noyes was neither his commander nor assigned to the Joint Staff Security Office ("JSSO"), which is responsible for personnel security matters.

Col Noyes used highly sensitive personal information from the file in a campaign to torpedo Lt Col Bigelow's career. Lt Col Bigelow was effectively fired from the Joint Staff, dropped from several top-flight military-run schools, and given a dead-end job at Bolling Air Force Base. For a time his promotion to Lieutenant Colonel was at risk. He was eventually transferred to Los Angeles Air Force Base, and retired on July 1, 2000.

---

[1] In the District Court, the parties cited to paragraphs in the internal DOD version of the Personnel Security Program regulation rather than the *Code of Federal Regulations*. *See, e.g.*, Pet. App. 27a-31a, 34a-37a, 93a. A Table of Parallel Provisions appears at page ix *supra*.

2. *Regulatory Framework*. Under the Privacy Act, otherwise nondisclosable records may be disclosed "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1).

Under DOD's regulations, "[r]ecords pertaining to an individual may be disclosed without the consent of the individual to any DOD official who has need for the record in the performance of his or her assigned duties." 32 C.F.R. § 310.41(a). Access to personnel security investigative reports shall be afforded only to persons whose official duties require such information. *Id.* § 154.65. Access to personnel security investigative reports and personnel security determination information can be authorized only in accordance with the Privacy Act Program and the Freedom of Information Act and, in pertinent part, with the following:

> Within DoD, access to personnel security investigative reports shall be limited to those designated DoD officials who require access in connection with *specifically assigned personnel* security duties, or other activities *specifically identified* under the provisions of [§ 154.65]. 32 C.F.R. § 154.67 (emphases added).

The Defense Security Service ("DSS", previously known as the Defense Investigative Service) is responsible for administration of the Personnel Security Investigations Program. It claims that "[a]ll information received during the course of the investigation is *scrupulously protected* under the laws and statutes of the U.S., including the Privacy Act of 1974." DSS, *Personnel Security Investigations, Frequently Asked Questions*, <www.dss.mil/aboutdss/faq. htm>, at 3 (emphasis

added). "In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with *the highest degree of discretion*. Access to such information shall be afforded only for the purposes cited herein and to persons whose official duties *require* such information." 32 C.F.R. § 154.65 (emphases added). The regulations also call for "internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records. . . ." *Id.* § 154.66.

3. *Lt Col Bigelow's DD Form 398*. In 1992, Lt Col Bigelow submitted a Personnel Security Questionnaire (DD Form 398) in order to obtain the Top Secret clearance required for assignment to the Joint Staff. Based upon the form and a personnel security investigation, the Air Force's Air Intelligence Agency, as the cognizant Central Adjudication Facility, determined that Lt Col Bigelow could have access to classified information. In turn, the JSSO determined that he had a need to know particular classified information.

4. *Privacy Act Violation*. In 1995, when Lt Col Bigelow was assigned to the Operations Branch of the Special Technical Operations Center, Col Noyes supervised him. Col Noyes was neither a "personnel security specialist" nor assigned to the JSSO. In the autumn of 1995, he learned of allegations of misconduct regarding Lt Col Bigelow. He met with the Air Force Office of Special Investigations, which declined to intervene. Then he contacted the JSSO, where he was permitted to examine Lt Col Bigelow's personnel security investigative report (which JSSO had illegally retained beyond the 90 days permitted by 32 C.F.R. § 154.69(a), Pet. App. 93a (¶ 7)). In this fashion he learned of other, unrelated

allegations that had been known to the responsible officials when Lt Col Bigelow was granted access to highly classified information.

Lt Col Bigelow was thereafter relieved of his duties and escorted from the Pentagon. A month later, he learned that Col Noyes had been permitted to examine his personnel security investigative report. In an effort to determine how Col Noyes had been able to obtain information protected by the Privacy Act, Lt Col Bigelow requested an accounting of all disclosures of his record while he was assigned to the Joint Staff. The Joint Staff Secretariat's Information Management Division (*not* the JSSO) responded that the disclosures were exempt from the Privacy Act's accounting requirement because they were made to officers and employees who had a need to know the information for the performance of their duties. Pet. App. 87a.

5. *Proceedings in the District Court.* Lt Col Bigelow sued DOD because JSSO had disclosed his security file to Col Noyes. The bases for federal jurisdiction in the District Court were the Privacy Act and 28 U.S.C. § 1331. He sought money damages for career and emotional harm; expungement of all reference to the matter that was disclosed; an accounting of all disclosures of his prior background investigations while he was assigned to the Joint Staff; attorney's fees and costs; and such other and further relief as might, in the circumstances, be just and proper.

Relying on an affidavit from Col Noyes and no other factual information regarding the disclosure at issue, DOD moved for summary judgment on the ground that he had a need to know the contents of Lt Col Bigelow's security file. Lt Col Bigelow sought limited discovery on several issues, such as Col Noyes's need to know, any procedure that provided for access by mere supervi-

sors, the identity and authority of the individual who permitted him to examine the file, and the connection between the disclosure and Lt Col Bigelow's reassignment. The District Court (Jackson, *J.*) granted summary judgment for DOD and denied Lt Col Bigelow's Rule 56(f) motion as moot. Pet. App. 25a. Ruling from the bench and explicitly (and impermissibly) drawing on intuition and personal experience as a naval officer (years before Congress passed the Privacy Act), the court found that because Col Noyes was Lt Col Bigelow's supervisor, he had the requisite need to know. Pet. App. 37a-38a.

No policy-level DOD official signed the government's brief. The only attorneys who entered appearances or signed anything in the District Court were from the United States Attorney's Office. No one from DOD's Office of General Counsel entered an appearance, signed anything, or even was shown as "of counsel." The name of a junior officer assigned to the Air Force's General Litigation Division was shown, without signature, as "of counsel" on a statement of points and authorities in support of a motion to dismiss or for summary judgment.

6. *Proceedings in the Court of Appeals.* The Court of Appeals denied cross-motions for summary disposition. After plenary briefing and argument, it ruled for DOD, holding, in an opinion by Judge Randolph, that Col Noyes' continual duty to assess the reliability and loyalty of subordinates gave him a "need to know" and that "[i]f we were somewhat less sure of our reading of the Defense Department's regulations, the interpretation advanced in the Department's brief would still carry the day," citing *Auer v. Robbins*, 519 U.S. 452, 462 (1997). Pet. App. 5a.

Judge Tatel dissented. In his view, "had the Secretary of Defense, exercising his authority to interpret Department regulations, interpreted 'shared' responsibility to mean that supervisors are 'designated DoD officials who require access in connection with specifically assigned personnel duties' within the meaning of section 154.67, I would defer to that interpretation," citing *Buffalo Crushed Stone, Inc. v. Surface Transp. Bd.*, 194 F.3d 125, 128 (D.C. Cir. 1999), "[b]ut neither the Secretary nor any other policy-making official has so interpreted the regulation." Pet. App. 9a-10a. Not only was there nothing in the record to demonstrate "that Noyes has authority to make policy for the Department," he "is the alleged wrongdoer in this case, the person with the greatest incentive to defend his past 'action[s] against attack,'" quoting *Auer* at 462. Pet. App. 11a-12a. "By deferring to [DOD's] brief, the court has not only dramatically expanded the number of people with a duty to examine highly sensitive personnel security files, but attributed to the Secretary an interpretation of section 154.60 that he cannot change without notice and comment rulemaking." Pet. App. 14a.

On petition for rehearing, Judge Tatel again dissented:

> Contrary to *Bowen v. Georgetown University Hospital*, the panel decision defers to "what appears to be nothing more than an agency's convenient litigating position." 488 U.S. 204, 213 (1988). Unlike in *Auer v. Robbins*, 519 U.S. 452, 461-63 (1997), and *Geier v. American Honda Motor Co.*, 120 S. Ct. 1913, 1926-27 (2000), the high-water marks of deference to litigating positions, here the agency's

own conduct is at issue and the proposed interpretation of section 154.60 was offered not only in defense of that conduct, but also for the first time in this case. Under such circumstances, the record must contain some evidence that the proposed interpretation reflects the agency's fair and considered judgment. Otherwise, the interpretation represents nothing more than a "*post-hoc* rationalization advanced . . . to defend past agency action against attack." *Auer*, 519 U.S. at 462.

To support its proposed interpretation of section 154.60, the government's brief cites only the affidavit of the very Department of Defense official whose conduct Bigelow challenges. The record, moreover, contains no evidence either of longstanding agency practice consistent with the government's interpretation of section 154.60 or of implicit agency reliance upon that interpretation, nor did Department of Defense attorneys sign the appellate brief. See *Bigelow*, 217 F.3d at 881. Although the government has now informed us that an Air Force lawyer's name appears as *of counsel* on the motion to dismiss in the district court, *see* Opposition to Appellant's Petition for Panel Rehearing and for Rehearing En Banc at 4, that is hardly sufficient to transform an interpretation of a regulation advanced for the first time as a defensive litigating position into a considered agency judgment worthy of deference. Pet. App. 22a-23a.

No DOD policy-level official with authority to interpret the regulations ever entered an appearance in the Court of Appeals, or signed or was shown, even as "of counsel," on the government's motion for summary affirmance or plenary brief. Nor did any of its submissions recite that Secretary Cohen had approved the interpretation asserted. The names of two attorneys in the Air Force's General Litigation Division were eventually shown (without signatures) as "of counsel" on the government's opposition to Lt Col Bigelow's rehearing petition.

Reasons for Granting the Petition

I

THE DECISION BELOW DRAMATICALLY EXPANDS THE CLASS OF PERSONS WHO MAY ACCESS OTHERS' SECURITY FILES AND MAKES A HASH OF THE DEFENSE DEPARTMENT'S PERSONNEL SECURITY PROGRAM REGULATION

1. The Personnel Security Program affects millions of citizens. Left undisturbed, the Court of Appeals' decision would grant to literally tens of thousands of DOD military and civilian supervisors a license to rummage. For this reason alone, if Judge Tatel is correct and the majority below erred, review here is essential.

The majority took issue with Lt Col Bigelow's claim—endorsed by Judge Tatel and not disputed by the government—that the District Court's decision would dramatically expand the number of people who would be under a duty to inspect others' security files. Nonetheless, the majority argued that

> [g]iven these circumstances it is an overstatement to suppose, as our dissenting colleague does, that our decision "has dramatically expanded the number of people" within the military who may examine personnel files. Dissenting op. at 881. There may be many people in the military who have access to the nation's most important secrets, but we doubt that their supervisors regularly receive information casting doubt on their trustworthiness. Pet. App. 4a-5a.

The clear implication is that the decision of the District Court (and, by extension, that of the Court of Appeals) is "no big thing." In addition to having nothing to do with whether the Privacy Act had been violated, this implication is simply untrue.

The Personnel Security Program applies to all members of the armed forces (other than the Coast Guard in peacetime), all civilian DOD employees, all defense contractor employees, and all "other personnel who are affiliated with" DOD. 32 C.F.R. § 154.2(b).[2] This describes literally millions of Americans.[3] "At the end of fiscal year 1998, about 2.4 million DOD active duty military, civilian, and contractor employees held personnel security clearances: 96,000 employees held

---

[2] The only exception is that unfavorable administrative action procedures for contractor personnel are separately prescribed in 32 C.F.R. Pt. 155.

[3] As of last year, there were 1.37 million military personnel on active duty, 1.35 in the ready and standby reserves, and 703,000 civilian DOD employees. DOD, *Defense Almanac* (1999), <www.defenselink.mil/pubs/almanac/>.

confidential clearances, 1.8 million held secret clearances, and 524,000 held top secret clearances." GAO, National Security and International Affairs Div., *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks* (Letter Report, Oct. 27, 1999, GAO/NSIAD-00-12), at 3.

The Court of Appeals majority's hunch that the supervisors of these millions do not "regularly receive information casting doubt on their trustworthiness" has absolutely no foundation. Given the sheer number of affected individuals, a regular flow of such cases seems highly likely, and such information as there is confirms this. DSS closed about 1,100 cases *per day* during the first quarter of FY 2000. GAO, *Audit Report, Security Clearance Investigative Priorities*, Rep. No. D-2000-11 (Apr. 5, 2000), at 6.[4] Looking only at one category of those covered by the regulation, "[a]pproximately 12,000 contractor cases a year are normally sent" from DSS to DOD's Office of Hearings and Appeals. Statement of Harold J. Kwalwasser, Dep. Gen. Counsel for Legal Counsel, DOD, Hearing before the Senate Comm. on Armed Services, Apr. 6, 2000, at 5, <www.senate.gov-/~armed_services/statemnt/2000/000406hk.pdf>.

The majority below also sought to downplay the magnitude of the change worked by its decision by

---

[4] The massive scale of the Personnel Security Program is apparent from the fact that the *backlog* of PRs was estimated earlier this year at 600,000. Statement of Carol R. Schuster, Assoc. Dir., National Security Preparedness Issues, National Security and International Affairs Div., GAO, Hearing before the Senate Comm. on Armed Services, Apr. 6, 2000, at 2, <www.senate.gov/~armed_services/statemnt/2000/000406cs.-pdf>; *see also* Edward T. Pound, *Security Clearance Backup Continues*, USA Today, Aug. 25, 2000, at 8A, col. 2 (noting interagency dispute over size of backlog).

treating as one of (if not *the*) operative circumstances (Pet. App. 4a) the fact that Col Noyes "had a need to examine the file in view of the doubts that had been raised in his mind about [Lt Col] Bigelow and [Lt Col] Bigelow's access to the country's top secrets."[5] This seriously misconceives the issue. Col Noyes's alleged need to know is said to have rested on a duty to monitor Lt Col Bigelow's trustworthiness. But that duty would have existed independent of any "doubts that had been raised in [Col Noyes's] mind." In other words, the scope of the change at issue must be gauged in light of the broader duty, whatever it was, rather than the particularized circumstance that Col Noyes had his doubts.[6]

---

[5] The Court of Appeals's citation to *Britt v. Naval Investigative Service*, 886 F.2d 544, 549 n.2 (3d Cir.), even with the telltale "*see*" signal and dictum parenthetical, Pet. App. 4a, is generous. Although the Third Circuit commented that disclosure of a criminal investigation file (not a security file) to a commanding officer (not a mere supervisor) "would appear to fall within the 'right [*sic*] to know' provision" of the Privacy Act, it made no effort to test the claimed need to know against the specifics of the applicable agency regulation, and noted that the disclosure was "no longer challenged."

[6] The majority's response to Judge Tatel's description of the sweeping effect of the decision subtly misstates an important element in his analysis. He properly assessed the impact of the decision in terms of supervisors' "*duty* to examine highly sensitive personnel security files," Pet. App. 14a (emphasis added), while the majority incorrectly paraphrases him (Pet. App. 4a) as having referred to "'the number of people' within the military who *may* examine personnel files." (Emphasis added.) By the majority's logic, that "may" is really a "must." As a result, the impact of the decision must be gauged against the entire class of supervisors, not merely whatever subset may at one time or another harbor doubts about a subordinate. Note also that it is not simply supervisors "in the military" who

2. On the merits, Judge Tatel described the majority's interpretation of the regulation as "counterintuitive." Pet. App. 7a. He was being charitable. Whether an individual has a Privacy Act "need to know" is not something that can be determined in the abstract, either by reference to intuition based on long-past personal experience (as Judge Jackson had done), Pet. App. 37a, or from other cases (as the majority did at least in part).[7] Rather, it depends upon the regulatory text, the philosophy underlying the regulations as stated by the issuing agency, and the particular individual's job. The Court of Appeals failed on all three counts.

DOD has established a complex system both for ensuring on a continuing basis that only those who are

---

would have such a duty; civilian DOD supervisors as well as defense contractor supervisory employees would be under the same duty.

[7] Because *Pippinger v. Rubin*, 129 F.3d 519, 529-30 (10th Cir. 1997), cited at Pet. App. 4a, involved the IRS, it adds nothing to the conversation insofar as the proper construction of DOD's regulation is concerned. Moreover, in direct contrast to the responsibilities said to have been imposed on the IRS employees to whom the information there at issue was disclosed, Col Noyes had no investigative function. Under DOD's regulation investigations are to be conducted by designated DOD subagencies. 32 C.F.R. §§ 154.9(a), -(c)(3). While *Hernandez v. Alexander*, 671 F.2d 402, 410 (10th Cir. 1982), also cited at Pet. App. 4a, arose within the Army, it makes no reference to DOD's Personnel Security Program regulation, and simply states conclusorily that "Lenko and Samaniego had need of plaintiff's EEO files in performance of their duties," which "included advising the White Sands [Missile Range] command group concerning personnel matters." Neither of them was a mere supervisor, *see id.* at 408-09, unlike Col Noyes, and the case had nothing to do with Hernandez's security file. With good reason the government never cited either of these cases below.

trustworthy may have access to the Nation's secrets and for safeguarding the highly sensitive personal information it must possess in order to achieve that first objective. Given the clear evidence that DOD intended the regulation to be part of a system that "scrupulously protect[s]" Privacy Act information and contemplates "the highest degree of discretion," *see* pp. 4-5 *supra*, those principles should have informed the Court of Appeals' analysis and led it to apply a hard look to any reading that defeats the statutory and regulatory protections and opens floodgates of access. Instead, the Court of Appeals majority read DOD's regulation loosely and without regard to the department's advertised purposes and orientation.

DOD's regulation goes into detail as to the role of supervisors. That role does not include snooping in others' security files even where the supervisor "has his doubts." If all supervisors indeed have a need to know the contents of their supervisees' security files, one would expect to find that simple proposition set forth *in haec verba* in agency regulations. But there is no hint of such a sweeping rule in the regulation DOD fashioned. Where the drafters intended to permit supervisors to have access to supervisees' security information, they did so explicitly and under narrow constraints.[8] Under the

---

[8] Section 154.60(c)(1) addresses supervisory responsibility for evaluating continued security eligibility:

> In conjunction with the submission of PR's [Periodic Reinvestigations, *see* § 154.3(q)] stated in § 154.19, and paragraph 5, Appendix A, supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's

familiar *expressio unius* canon of construction, *e.g.*, *Christensen v. Harris County*, 120 S. Ct. 1655, 1660-61 (2000); *O'Melveny & Myers v. F.D.I.C.*, 512 U.S. 79, 86 (1994), the fact that the regulation limits supervisor access with such particularity disposes of the notion that supervisors enjoy a roving commission to access subordinates' entire security files.

The regulation includes a variety of express provisions that rule out vigilante action like Col Noyes's. Personnel security investigations are the exclusive province of DSS.[9] Allegations of possible criminal activity, are carved out of the mandatory referral to DSS, 32 C.F.R. §§ 154.9(c)(3)-(4), and must be referred, in the case of uniformed personnel, to the appropriate Military Criminal Investigative Organization. *Id.* § 154.9(c)(4). Under § 154.9(c)(3), which is especially pertinent because it concerns personnel security investigations conducted *after* there has been a determination of an

---

> continued eligibility for access to classified information is omitted.

Col Noyes's access was not authorized under this provision because his review of Lt Col Bigelow's security file was not confined to DD Form 398, which is merely a questionnaire completed by the individual seeking a clearance. Col Noyes was permitted to examine Lt Col Bigelow's *entire* security file, including raw investigative data. Moreover, Col Noyes's review was not "[i]n conjunction with the submission of" a PR.

[9] DSS "provides a single centrally directed personnel security investigative service to conduct personnel security investigations within the 50 States, District of Columbia, and Commonwealth of Puerto Rico. . . . *No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Under Secretary of Defense for Policy.*" 32 C.F.R. § 154.9(a) (emphasis added).

individual's eligibility for access to classified information or retention in a sensitive position, derogatory suitability allegations "shall be referred to [DSS] to conduct a Special Investigative Inquiry." Self-help by every supervisor is simply not part of this pervasively regulated field.

Under the heading "Continuing Security Responsibilities," the regulation provides that "[t]he responsibility for [continuing assessment of trustworthiness after a clearance has been issued] must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself." *Id.* § 154.60(a). But the term "share" is clearly used only to recognize that a number of officials may be involved in the overall process of continuing assessment, not to say that there are no boundary lines that distinguish the individual roles of the participants. Col Noyes's "share" in the "shared responsibility" was to refer allegations of misconduct to his commander to determine whether investigation was called for.

The Court of Appeals majority's reliance on § 154.55(b)(1)[10] is entirely misplaced. That section merely calls for derogatory information to be reported to the proper authority. It is perverse to read this duty to report information that is "developed" or "become[s] 'available'" as carrying within it an affirmative, antecedent obligation to *search out* such information even if

---

[10] Whenever derogatory information relating to the criteria and policy set forth in § 154.7(a) and Appendix H of this part is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty.

that information is, as here, already in the hands of security personnel. If Col Noyes had "doubts," his duty was to report them to those responsible for investigation.

3. Allowing a supervisor—even one with "doubts"—to rummage in the sensitive files held by the JSSO makes a hash of the process and the institutional relationships established by DOD's regulation. Under § 154.55(b)(1), derogatory information must be referred to either the security office—here, the JSSO—or the commander. Under the Court of Appeals majority's reading, if a supervisor, having been permitted to review others' security files held by the security office, found something he thought was derogatory, he would have to do one of two things: refer it to the security officer or refer it to the commanding officer. It obviously makes no sense to refer something to the security office that is already in that office's ken. And for a supervisor—not assigned to the security office—to refer matter he has seen in that office's own files to the commanding officer would permit every supervisor to second-guess the trained experts and interject himself between the security officer and the commanding officer. Either way, the majority's view of the duties of a supervisor subverts the regulation's careful allocation of tasks, not to mention DOD's assurances that investigative information will be "scrupulously protected" and handled "with the highest degree of discretion." The regulation, as Judge Jackson observed, may be "turgid," Pet. App. 37a, but it still deserves far more respectful treatment than the majority below afforded it.

4. Even now, it is unclear that *anyone* at the JSSO actually made the requisite need to know determination. Although Col Noyes, who was not assigned to the

JSSO, claimed he had a need to know the contents of Lt Col Bigelow's security file, Pet. App. 90a (¶ 6), nothing in his declaration indicates that he explained the factual basis for that claim to the person who afforded him access to the file. *Id.* (¶ 5). Describing his interaction with the JSSO, Col Noyes states:

> (5) Consequently, I went to the [JSSO] and requested Major Bigelow's personnel security file because it was my considered opinion that he was lying about certain aspects of his past. The procedure is such that a personnel security specialist will access the file and then review it with the supervisor, provided that the supervisor has the appropriate clearance level, which I did. . . . *Id.*

But he never says that the security specialist made a need to know determination or even was made aware of the facts on which Col Noyes claims to have had a need to know. Tellingly, the government never submitted anything from the JSSO in support of its motion for summary judgment. Both aspects of the case—Col Noyes's claimed need to know and judicial deference to a *post hoc* rationalization, *see* Point II *infra*—thus share a fatal defect: the record contains nothing from a competent agency official as to either one.

While the District Court rules *de novo* when an agency asserts a need to know defense, the judicial process would plainly benefit if the court were able to review the custodian's statement of the facts that were taken into account at the time of disclosure. "The releasing official, normally the records custodian, should determine whether it is a valid agency function and whether the information is actually needed to perform

the function." John F. Joyce, *The Privacy Act: A Sword and a Shield But Sometimes Neither*, 99 MIL. L. REV. 113, 147 (1983). Without a statement from that official, the court is placed in the unacceptable position of having to take a possible wrongdoer's self-serving word and, in the sense that the main player (the records custodian) was AWOL, allow *Hamlet* to proceed without the Prince. *Cf. Kargman v. Sullivan*, 552 F.2d 2, 4 (1st Cir. 1977); *Tampa Phosphate R.R. v. Seaboard Coast Line R.R.*, 418 F.2d 387, 396 n.6 (5th Cir. 1969), *cert. denied*, 397 U.S. 910 (1970).

Admittedly, DOD is a party here, but the individual who allowed Col Noyes to examine Lt Col Bigelow's file (and had a duty to make a need to know determination before doing so) has never even been identified, much less submitted a sworn statement that Lt Col Bigelow could test through normal discovery. Without knowing that individual's rank, for example, it is impossible to determine whether Col Noyes's seniority permitted him to exert undue influence over the custodian. *Cf. Meehan v. Macy*, 392 F.2d 822, 838 (D.C. Cir. 1967) ("as the Ensign said to the Admiral, 'Your every wish is my command'"), *modified*, 425 F.2d 469 (1968), *reinstated in part*, 425 F.2d 472 (1969) (en banc) (per curiam).

The need for *something* from the official responsible for maintaining security files is further underscored by the government's repeated insistence that "even if Colonel Noyes went unsupervised into the security office through a window in the dead of night to review the files in violation of a hundred written procedures, he still had a 'need for the record.'"[11] The use of stealth

---

[11] Motion for Summary Reversal at 6 n.6; Opp. to Pl. Motion to Conduct Limited Discovery at 5.

or other unauthorized procedures would be highly probative, albeit circumstantial, evidence that he did not in fact have a need to know. Requiring a statement from the custodian would help identify cases in which release was irregular.

For these reasons, DOD's evidentiary submission was inadequate to support summary judgment and it was improper to deny Lt Col Bigelow the basic discovery to which every litigant is entitled.

II

THE DECISION BELOW CONFLICTS WITH *BOWEN* BECAUSE IT DEFERS TO AN INTERPRETATION THAT HAS NEVER BEEN ANNOUNCED OR EMBRACED BY ANY POLICY-LEVEL OFFICIAL

Perhaps sensing that its own analysis was insufficient to carry the day, the majority below claimed that even if it "were somewhat less sure of [its] reading of the Defense Department's regulations, the interpretation advanced in the Department's brief would still carry the day." Pet. App. 5a. As Judge Tatel explained, however, reliance on that interpretation conflicts with *Bowen*. *See also, e.g., Martin v. OSHRC*, 499 U.S. 144, 156 (1991); Pet. App. 7a, 10a-12a, 22a. This is not a case in which deference is owed to an agency's interpretation of its own regulation: here there has been no such interpretation. Neither Col Noyes nor the United States Attorney's Office is competent to issue a deference-incurring interpretation. Col Noyes was not assigned to security duties and there is no reason to treat his claim that he had a need to know as anything other than a personal view. What is more, since it is his conduct that is at issue, his claim (which Lt Col Bigelow was never allowed

to test through discovery) is transparently self-serving.

As an Army officer (one of thousands), Col Noyes at least was part of the Defense Department. The United States Attorney's Office cannot even claim this status. Nor can it claim that its submissions here and below reflect a "fair and considered" agency judgment, *Auer, supra*, 519 U.S. at 462, since at no time during this litigation has *any* policy-level official publicly evinced concurrence with the views that have been asserted in DOD's name.

The Court of Appeals majority's reliance on *Auer* in preference to *Bowen* is unjustified. In addition to the reasons advanced by Judge Tatel, the agency interpretation to which this Court deferred in *Auer*, even though it was articulated in the course of the litigation, had vastly firmer indicia of agency-level approval than does the reading adopted below at the behest of the United States Attorney's Office. Specifically, the government position there was not only affirmatively requested by the Court, 516 U.S. 1109 (1996) (mem.), and understood to be the views of the Secretary of Labor, 519 U.S. at 461, but its brief *amicus curiae* bore the names of Acting Solicitor (and Assistant Secretary) of Labor J. Davitt McAteer and other Department of Labor attorneys above those of the Acting Solicitor General, his Deputy and the Assistant who argued the case. Brief for the United States as Amicus Curiae, *Auer v. Robbins*, 1995 U.S. Briefs 897 [LEXIS], No. 95-897 (U.S.).[12]

---

[12] In the airbags case, where the majority thought "the agency's views should make a difference," *Geier, supra*, 120 S. Ct. at 1926-27; *compare id.* at 1941 (Stevens, J., dissenting), the government's position was of long standing and its brief bore the names, among others, of the General Counsel of the Department of Transportation and the Chief Counsel of the National

Conclusion

The petition for a writ of certiorari should be granted.

Respectfully submitted,

EUGENE R. FIDELL
(Counsel of Record)
DAVID P. SHELDON
JAMES L. FELDESMAN
FELDESMAN, TUCKER, LEIFER,
FIDELL & BANK LLP
2001 L Street, N.W.
Washington, D.C. 20036
(202) 466-8960

Attorneys for Petitioner

DECEMBER 2000

Highway Traffic Safety Administration. Brief for the United States as Amicus Curiae Supporting Affirmance, *Geier v. American Honda Motor Co., Inc.*, No. 98-1811, <www.usdoj-.gov/osg/briefs/1999/3mer/1ami/98-1811/mer.ami.html>,

APPENDIX

TABLE OF CONTENTS

	Page
Decision of the Court of Appeals (July 14, 2000)	1a
Judgment of the Court of Appeals (July 14, 2000)	15a
Order denying rehearing (Oct. 13, 2000)	17a
Order denying rehearing *En Banc* (Oct. 13, 2000)	18a
Order amending Judge Tatel's dissent from denial of rehearing and rehearing *en banc* (Oct. 25, 2000)	20a
Statement of Judge Tatel dissenting from denial of rehearing and rehearing *en banc* (corrected version)	22a
Judgment of the District Court (June 11, 1999)	24a
Order (June 11, 1999)	25a
Transcript of proceedings in the District Court (June 11, 1999)	26a
Privacy Act of 1974, 5 U.S.C. § 552a (1994) (excerpts)	40a
Dep't of Defense Personnel Security Program, 32 C.F.R. Pt. 154 (2000) (excerpts)	58a
§ 152.2	58a
§ 154.3	58a
§ 154.9	65a
§ 154.47	69a
§ 154.55	70a
§ 154.56	75a
§ 154.60	77a
§ 154.65	81a
§ 154.66	82a
§ 154.67	82a
§ 154.68	83a
§ 154.69	84a

Dep't of Defense Privacy Program,
32 C.F.R. Pt. 310 (2000) (excerpt) 86a
§ 310.41(a) 86a
Letter from Edmund F. McBride, Chief,
Information Management Division,
Secretariat, Joint Staff (Aug. 19, 1997) 87a
Declaration of Col Nathan W. Noyes
(June 11, 1998) 89a
Affidavit of Steven D.C. Bigelow in Support of
Plaintiff's Motion to Conduct Limited Discovery
(July 24, 1998) 91a

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued May 17, 2000 Decided July 14, 2000

No. 99-5280

Steven D.C. Bigelow, *Appellant*

v.

Department of Defense, *Appellee*

Appeal from the United States District Court
for the District of Columbia
(98cv00535)

Eugene R. Fidell argued the cause for appellant. With him on the briefs was *David P. Sheldon*.

W. Mark Nebeker, Assistant U.S. Attorney, argued the cause for appellee. With him on the brief were *Wilma A. Lewis*, U.S. Attorney, and *R. Craig Lawrence*, Assistant U.S. Attorney.

Before: GINSBURG, RANDOLPH, and TATEL, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* RANDOLPH.

Dissenting opinion filed by *Circuit Judge* TATEL.

RANDOLPH, *Circuit Judge*: Steven D.C. Bigelow, while a major in the United States Air Force, worked in the Information Warfare and Special Technical Operations Center, a part of the Office of the Joint Chiefs of Staff in the Pentagon. The chief of that section and Major Bigelow's immediate supervisor, United States Army Colonel Nathan W. Noyes, learned of allegations of misconduct concerning Bigelow, perhaps the most serious of which was that he sometimes disappeared in foreign countries near sensitive international borders. Major Bigelow's position demanded that he hold the highest security classification, above "Top Secret" (the name of the classification is itself classified). Colonel Noyes's position, so it is claimed, demanded that he continually assess the trustworthiness of those under his command. To this end, and because he thought Bigelow might be lying about his past, Noyes went to the Joint Staff Security Office and requested Bigelow's personnel security file. Convinced that his suspicions had been confirmed, Colonel Noyes referred the matter to the Air Force for disciplinary action, as a result of which Major Bigelow was relieved of his duties at the Pentagon (he is now a Lieutenant Colonel at Bolling Air Force Base).

Bigelow brought this action under the Privacy Act, 5 U.S.C. § 552a, seeking damages and other relief against the Department of Defense on the ground that Colonel Noyes unlawfully reviewed his personnel security file in violation of the Act. The district court, Judge Thomas P. Jackson, granted the government's motion for summary judgment and declared moot Bigelow's motion for discovery pursuant to Rule 56(f) of the Federal Rules of Civil Procedure.

The appeal comes down to the question whether Colonel Noyes, as an officer of the agency maintaining

the file, had "a need for the [Bigelow's] record in the performance of [his] duties." 5 U.S.C. § 552a(b)(1). Among other things the Privacy Act generally prohibits government agencies from disclosing personnel files. To this general prohibition there are several exceptions, one of which is the "need-to-know" provision of § 552a(b)(1). The Defense Department assures us, through a brief filed on its behalf by the United States Attorney, and through a sworn declaration of Colonel Noyes, that Noyes's duties entailed examining Bigelow's personnel security file because Bigelow was under his supervision. We believe the Department's regulations support this position.

At the Pentagon, "personnel security investigative reports" may be revealed only to "those designated DoD officials who require access in connection with specifically assigned personnel duties, or other activities specifically identified under the provisions of s 154.65." 32 C.F.R. § 154.67. The activities mentioned in § 154.65 include "determining eligibility of DoD military and civilian personnel . . . [for] assignment or retention in sensitive duties." 32 C.F.R. § 154.65. Major Bigelow had "access to the Nation's most sensitive secrets." Amended Complaint ¶ 45. Did Colonel Noyes have a continuing duty to determine whether Major Bigelow should be retained in his sensitive duties on the Joint Chiefs of Staff? According to § 154.60(a) of the regulations, the answer is yes. An "individual's trustworthiness is a matter of continuing assessment," and the "responsibility for such assessment must be shared by the organizational commander or manager, [and] the individual's supervisor. . . ." 32 C.F.R. § 154.60(a).

Bigelow and our dissenting colleague read § 154.60(a) differently than does the Defense Department.

Judge Tatel asserts that despite the unconditional wording of § 154.60(a), military supervisors do not have an official need to examine personnel files in assessing the trustworthiness of any individual under their command. Why not? Because only commanders and security officers have access to personnel security files, which of course begs the question. Bigelow, at least, is willing to concede that a supervisor is responsible for assuring the trustworthiness of those under him. The question is how the supervisor may go about this. Bigelow says that the various ways of fulfilling the supervisor's duty are spelled out in § 154.60(c). Searching personnel files for derogatory information is not listed. We think his line of reasoning misses the point of the need-to-know exemption in the Privacy Act. Section 552a(b)(1) does not require an agency to list those of its officers eligible to look at protected records, nor does it demand that an agency official be specifically assigned to examining records. What must be determined—and what Judge Tatel does not confront—is whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly. *See Pippinger v. Rubin*, 129 F.3d 519, 529-30 (10th Cir. 1997); *Hernandez v. Alexander*, 671 F.2d 402, 410 (10th Cir. 1982). Colonel Noyes reviewed Major Bigelow's file in connection with his continuing duty to make sure that the major was worthy of trust; and he had a need to examine the file in view of the doubts that had been raised in his mind about Bigelow and Bigelow's access to the country's top secrets. *See Britt v. Naval Investigative Service*, 886 F.2d 544, 549 n.2 (3d Cir. 1989) (dictum). Given these circumstances it is an overstatement to suppose, as our dissenting colleague does, that our decision "has dramatically expanded the number of people" within the military who may examine personnel files. Dissenting op. at 881.

There may be many people in the military who have access to the nation's most important secrets, but we doubt that their supervisors regularly receive information casting doubt on their trustworthiness.

Bigelow points to § 154.55, which gives commanders, upon the receipt of certain kinds of "derogatory information" about an individual, the power to take actions including temporarily suspending the individual's access to classified materials in the interest of national security. 32 C.F.R. § 154.55(c). Although Colonel Noyes was the "Chief" of his unit, all agree that he was not a commander within the regulation's intent. Still, we cannot see how this regulation helps Bigelow's case. From all that appears, § 154.55, together with its procedural counterpart (32 C.F.R. § 154.56), simply spells out in detail the formal administrative adjudicatory scheme for revoking or suspending security clearances. The regulation nowhere mentions who shall have access to personnel security records; that is the subject of § 154.65 and § 154.67, which we have already cited. It does not relieve supervisors of their duty, spelled out in § 154.60(a), to assess continually the reliability and loyalty of those working under them. While § 154.55(b) does require the reporting of "derogatory information" to the commander forthwith, it contemplates that such information will first be "developed" or will become "available." 32 C.F.R. § 154.55(b). Here Colonel Noyes developed such information and when he reported it to the Air Force, as he attests in his affidavit, he presumably acted in accordance with § 154.55(b).

If we were somewhat less sure of our reading of the Defense Department's regulations, the interpretation advanced in the Department's brief would still carry the day. Although the Supreme Court held in *Christensen v.*

Harris County, 120 S. Ct. 1655, 1662-63 (2000), that agency interpretations of statutes must derive from some formal agency action before judicial deference is due, the Court treated *Auer v. Robbins*, 519 U.S. 452, 462 (1997), as still good law despite the fact that the agency's interpretation—there of a regulation—appeared only in a legal brief. *Auer* does not require an agency to demonstrate affirmatively that its interpretation represents its fair and considered judgment. *See id.* Nor must an agency's litigating position represent some "long-standing agency practice." Dissenting op. at 881 (quoting *Akzo Nobel Salt, Inc. v. FMSHRC*, 212 F.3d 1301, 1304 (D.C. Cir. 2000)). *Auer* held that so long as there is no basis to suspect that the agency's position represents anything less than its considered opinion, deference is appropriate. *Auer* put the matter in these terms: the Court had "no reason to suspect that the interpretation does not reflect the agency's fair and considered judgment." 519 U.S. at 462. Like the *Auer* Court, we have no reason to suppose that the interpretation of the regulations set forth by government counsel represents anything other than his client's position. And we have been pointed to no past practices or pronouncements that are inconsistent with the Defense Department's current interpretation. *Compare Akzo Nobel Salt, Inc.*, 212 F.3d at 1305 (finding deference unwarranted given "the flip-flops [in] the Secretary's position. . . . [and] litigation counsel's simultaneous advocacy of several different positions"). The Department's interpretation of the regulations is therefore entitled to weight.

Because we are unpersuaded that discovery would have reaped anything pertinent to resolving these issues, we will not upset the district court's discretionary decision to refuse to grant Major Bigelow's Rule 56(f) motion before acting on the motion for summary judg-

ment. *See White v. Fraternal Order of Police*, 909 F.2d 512, 517 (D.C. Cir. 1990).

Affirmed.

TATEL, *Circuit Judge, dissenting*: To maintain national security, Department of Defense employees whose official duties require access to classified information undergo extensive, very personal background investigations. The regulatory scheme at issue in this case protects the sensitive information collected during those investigations and maintained in personnel security files—information about political associations, criminal or dishonest conduct, mental illness, family relationships, financial circumstances, drug and alcohol use, sexual behavior, etc. *See* 32 C.F.R. § 154.7 & Pt. 154, App. H. Relying on the government's appellate brief in this case, which in turn relies solely on a declaration of the non-policymaking employee whose behavior is the target of this suit, this court interprets the regulations to give access to personnel files not just to officials specified in the regulation, but to any supervisor anywhere in the Department who doubts an employee's loyalty. Because there is more than ample "reason to suspect" that this counterintuitive interpretation of the regulation represents a convenient litigating position rather than the "fair and considered judgment" of the Secretary of Defense or any other official with policy-making responsibility, *Auer v. Robbins*, 519 U.S. 452, 462 (1997), Supreme Court and circuit precedent preclude us from deferring to it. *See, e.g., Bowen v. Georgetown Univ. Hospital*, 488 U.S. 204, 213 (1988); *Akzo Nobel Salt v. FMSHRC*, 212 F.3d 1301 (D.C. Cir. 2000).

The Privacy Act prevents non-consensual release of personnel records except "to those officers and

employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). Reinforcing this protection, Defense Department regulations provide:

> In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information be handled with the highest degree of discretion. Access to such information shall be afforded only for the purposes cited herein and only to persons whose official duties require such information.

32 C.F.R. § 154.65. To protect the privacy of personnel security files, the regulation requires them to be stored only in approved locked cabinets, vaults, or safes; transmitted only in sealed double envelopes bearing a special restricted access notation; and reproduced only to the minimum extent necessary. *See id.* § 154.68. Information contained in these files may not be made available without the consent of the subject except to those personnel who have an official need for the information, and then only for specified limited purposes: "determining eligibility . . . for access to classified information, assignment or retention in sensitive duties, . . . or for law enforcement and counterintelligence investigations." *Id.* § 154.65. Commanders and security officers who have "specifically assigned personnel security duties" may access the files. *Id.* § 154.67(b). But "[r]ank, position, or title alone do not authorize access to personal information about others. An official need for the information must exist before disclosure." *Id.* § 310.41(a)(2).

Despite these regulatory safeguards, Colonel Noyes obtained Major Bigelow's file solely on the basis of his status as Bigelow's supervisor. The government does not contend that Noyes has any law enforcement, counterintelligence, or other "specifically assigned personnel security duties." *Id.* § 154.67(b). Nor does it claim that Noyes is one of the specifically enumerated persons empowered to make decisions about Bigelow's security clearance or duty assignment. *See id.* Pt. 154, App. E; § 154.47(b); § 154.55(c). Indeed, the regulations make it quite clear that if Noyes was "aware of . . . significant adverse information" about Bigelow, his obligation was to forward that information to the Defense Investigative Service for further investigation. *Id.* § 154.60(c)(3). That agency, not Noyes, was responsible for reviewing the information and determining whether Bigelow's conduct required further investigation. *Id.* § 154.9 ("No other DoD component [other than the Defense Investigative Service] shall conduct personnel security investigations unless specifically authorized by the Deputy Under Secretary of Defense for Policy.")

Citing section 154.60 of the regulations, my colleagues conclude that Noyes had an "official need" for access to Bigelow's file because "[a]n 'individual's trustworthiness is a matter of continuing assessment,' and the 'responsibility for such assessment must be shared by the organizational commander or manager, [and] the individual's supervisor' "—in this case, Noyes. Maj. Op. at 877 (quoting 32 C.F.R. § 154.60(a)). Although I agree with my colleagues that the regulations impose on supervisors a "shared" duty to assess the trustworthiness of those they supervise, I do not agree that this duty gives supervisors a per se "official need"—indeed duty—to go through security files. The regulations protect the privacy of personnel security files by

providing access only to certain specified officials (commanders and security officers) and by requiring that supervisors like Noyes report their concerns to the Defense Investigative Service for further investigation. 32 C.F.R. § 154.60(c)(3). Of course, had the Secretary of Defense, exercising his authority to interpret Department regulations, interpreted "shared" responsibility to mean that supervisors are "designated DoD officials who require access in connection with specifically assigned personnel duties" within the meaning of section 154.67, I would defer to that interpretation. *See Buffalo Crushed Stone v. Surface Transp. Bd.*, 194 F.3d 125, 128 (D.C. Cir. 1999) ("Where the meaning of regulatory language is not free from doubt, we will defer to the agency's interpretation so long as it sensibly conforms to the purpose and wording of the regulations.") (internal quotation marks and alteration omitted). But neither the Secretary nor any other policy-making official has so interpreted the regulation.

The Supreme Court made clear in *Auer* that under certain circumstances we may defer to regulatory interpretations that appear "only in the context of" litigation. 519 U.S. at 462. But *Auer* deference has limits. In *Bowen*, the Supreme Court held that "[d]eference to what appears to be nothing more than an agency's convenient litigating position would be entirely inappropriate." 488 U.S. at 213. The difference between the two cases is this—the Court deferred to the Secretary's interpretation in *Auer* because, unlike in *Bowen*, it was "in no sense a post hoc rationalization advanced by an agency seeking to defend past agency action against attack," but instead "reflect[ed] the agency's fair and considered judgment on the question." *Auer*, 519 U.S. at 462 (internal quotation marks and citation omitted). *See also Martin v. OSHRC*, 499 U.S. 144, 156

(1991) ("Our decisions indicate that agency litigating positions are not entitled to deference when they are merely appellate counsel's *post hoc* rationalizations for agency action, advanced for the first time in the reviewing court.") (internal quotation marks omitted); *Akzo Nobel Salt*, 212 F.3d at 1304 ("[C]ourts . . . defer to agency interpretations of ambiguous regulations first put forward in the course of litigation, but only where they 'reflect the agency's fair and considered judgment on the matter in question.'") (quoting *Auer*, 519 U.S. at 462). This insistence that an agency exercise its "fair and considered judgment" stems from two concerns: "First, appellate counsel's interpretation may not reflect the views of the agency itself. Second, it is likely that 'a position established only in litigation may have been developed hastily, or under special pressure,' and is not the result of the agency's deliberative processes." *National Wildlife Fed'n v. Browner*, 127 F.3d 1126, 1129 (D.C. Cir. 1997) (quoting *FLRA v. United States Dept. of Treasury*, 884 F.2d 1446, 1455 (D.C. Cir. 1989)). Thus, we may defer to an agency's litigating position if, for instance, it merely "articulate[s] an explanation of longstanding agency practice," *Akzo Nobel Salt*, 212 F.3d at 1304 (citing *Association of Bituminous Contractors, Inc. v. Apfel*, 156 F.3d 1246, 1252 (D.C. Cir. 1998)), or if the Secretary explicitly adopts the position expressed in the brief, *see FLRA*, 884 F.2d at 1455, but not where the record "strongly suggests to us that the Secretary has in fact never grappled with—and thus never exercised her judgment over—the conundrum posed by the regulation's clear ambiguity." *Akzo Nobel Salt*, 212 F.3d at 1305.

Bowen, not *Auer*, controls this case. The record indicates that the Secretary of Defense has never "grappled with" or "exercised [his] judgment over . . . the

conundrum posed by [this] regulation's clear ambiguity": whether all supervisors have a per se duty to review the personnel security files of employees they supervise. *Id.* The government's brief cites only one source in support of its interpretation of the regulation: a declaration prepared for this litigation by Noyes. Nothing in the record, however, demonstrates that Noyes has authority to make policy for the Department. *See Paralyzed Veterans of America v. D.C. Arena L.P.*, 117 F.3d 579, 587 (D.C. Cir. 1997) ("A speech of a mid-level official of an agency . . . is not the sort of 'fair and considered judgment' that can be thought of as an authoritative departmental position.") (quoting *Auer*, 519 U.S. at 462). Indeed, the statement in Noyes's declaration cited in the brief—"I had an official need to know the information in the personnel security file of any employee under my supervision in order to protect the interests of national security"—does not purport to set agency policy. It represents only Noyes's view about why he thought he had authority to search Bigelow's file. Noyes, moreover, is the alleged wrongdoer in this case, the person with the greatest incentive to defend his past "action[s] against attack." *Auer*, 519 U.S. at 462.

Of course, we could rely on the government's appellate brief alone if its interpretation of the regulation reflected the agency's "fair and considered judgment." *Auer*, 519 U.S. at 462 (deferring to the Secretary of Labor's explicit interpretation of his regulation appearing for the first time in her amicus brief). But it does not. The brief merely asserts that "Appellee" has interpreted its regulation to require supervisors to review personnel files, citing only the Noyes declaration. Moreover, the record contains none of the indicators that would allow us to conclude that a government position set forth for the first time in an appellate brief

reflects an agency's "fair and considered judgment." The brief does not say that the Defense Department has a "longstanding agency practice" of allowing supervisors access to personnel files, *Akzo Nobel Salt*, 212 F.3d at 1304, nor is there any indication that the Department "in practice . . . has, at least implicitly, followed the same interpretation that it advances on appeal." *National Wildlife Fed'n*, 127 F.3d at 1129. Defense Department lawyers, moreover, neither signed the brief nor appear of counsel, as agency lawyers often do in our cases. *See FLRA*, 884 F.2d at 1455 (deferring to agency interpretation in brief because "Ms. Horner, the agency head, has explicitly adopted the view of the amicus brief. There is no risk that counsel may have acted as mavericks disembodied from the agency that they represent.") (internal quotation marks omitted).

It misses the point to say that "we have been pointed to no past practices or pronouncements that are inconsistent with the Defense Department's current interpretation." Maj. Op. at 878. The point is that we have good "reason to suspect that this interpretation does not reflect the agency's fair and considered judgment" (*Auer*'s words) and is nothing more than the position of the U.S. Attorney and the two AUSAs who signed the brief. As the Supreme Court observed in a similar situation where counsel "rationalized the basis of [a regulation] with great professional competence. . . . this is hardly tantamount to an administrative interpretation of [the relevant statutory provisions]. . . . Congress has delegated to the administrative official and not to appellate counsel the responsibility for elaborating and enforcing statutory commands." *Investment Co. Inst. v. Camp*, 401 U.S. 617, 628 (1971). And as we said in *City of Kansas City, Missouri v. HUD*, 923 F.2d 188, 192 (D.C. Cir. 1991), "[i]n whatever context we defer to

agencies, we do so with the understanding that the object of our deference is the result of agency decision-making, and not some post hoc rationale developed as part of a litigation strategy."

For these reasons, I believe that the U.S. Attorney's brief represents a classic example of "'*post hoc* rationalization[ ]' advanced by an agency seeking to defend past agency action against attack." *Auer*, 519 U.S. at 462. By deferring to the brief, the court has not only dramatically expanded the number of people with a duty to examine highly sensitive personnel security files, but attributed to the Secretary an interpretation of section 154.60 that he cannot change without notice and comment rulemaking. *See Paralyzed Veterans of America*, 117 F.3d at 586 ("Once an agency gives its regulation an interpretation, it can only change that interpretation as it would formally modify the regulation itself: through the process of notice and comment rulemaking."). I respectfully dissent.

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 99-5280 September Term, 1999

Steven D.C. Bigelow, Appellant

v.

Department of Defense, Appellee

Appeal from the United States District Court
for the District of Columbia
(No. 98cv00535)

Before: GINSBURG, RANDOLPH and TATEL, *Circuit Judges*.

JUDGMENT

This cause came on to be heard on the record on appeal from the United States District Court for the District of Columbia and was argued by counsel. On consideration thereof, it is

ORDERED and ADJUDGED, by the Court, that the judgment of the District Court appealed from in this cause is hereby affirmed, in accordance with the opinion for the Court filed herein this date.

FOR THE COURT
Mark J. Langer, Clerk

BY: /s/
Robert A. Bonner
Deputy Clerk

Date: July 14, 2000

Opinion for the Court filed by Circuit Judge Randolph.
Dissenting opinion filed by Circuit Judge Tatel.

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 99-5280 September Term, 2000
98cv00535

Filed On: OCT 13 2000 [stamp]

Steven D.C. Bigelow, Appellant

v.

Department of Defense, Appellee

BEFORE: Ginsburg, Randolph and Tatel, Circuit Judges.

ORDER

Upon consideration of appellant's petition for rehearing filed August 28, 2000, and of the response thereto, it is

ORDERED that the petition be denied.

Per Curiam

FOR THE COURT
Mark J. Langer, Clerk

BY: /s/
Robert A. Bonner
Deputy Clerk

Circuit Judge Tatel would grant the petition for rehearing.

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 99-5280 September Term, 2000
98cv00535

Filed On: OCT 13 2000 [stamp]

Steven D.C. Bigelow, Appellant

v.

Department of Defense, Appellee

BEFORE: Edwards, Chief Judge; Silberman, Williams, Ginsburg, Sentelle, Henderson, Randolph, Rogers, Tatel and Garland, Circuit Judges.

ORDER

Appellant's petition for rehearing en banc and the response thereto have been circulated to the full court. The taking of a vote was requested. Thereafter, a majority of the judges of the court in regular active service did not vote in favor of the petition. Upon consideration of the foregoing, it is

ORDERED that the petition be denied.

Per Curiam

FOR THE COURT
Mark J. Langer, Clerk

BY: /s/
Robert A. Bonner
Deputy Clerk

A statement of Circuit Judge Tatel dissenting from the denial of rehearing is attached.

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 99-5280 September Term, 1999

FILED OCT 25 2000 [stamp]

Steven D.C. Bigelow, Appellant

v.

Department of Defense, Appellee

Appeal from the United States District Court
for the District of Columbia
(No. 98cv00535)

Before: EDWARDS, *Chief Judge*; SILBERMAN, WILLIAMS, GINSBURG, SENTELLE, HENDERSON, RANDOLPH, ROGERS, TATEL and GARLAND, *Circuit Judges*.

ORDER

It is ORDERED that the statement of Judge Tatel dissenting from the denial of rehearing *en banc*, attached to the Court's Order denying rehearing *en banc*, filed October 13, 2000, is amended as follows:

At lines 6 and 7 of the second paragraph, replace the words "lawyer signed" with "lawyer's name appears as *of counsel* on."

FOR THE COURT:
Mark J. Langer, Clerk

BY: /s/
Deputy Clerk

[Corrected Version]

Statement of TATEL, *Circuit Judge*, dissenting from the denial of rehearing and rehearing *en banc*:

Contrary to *Bowen v. Georgetown University Hospital*, the panel decision defers to "what appears to be nothing more than an agency's convenient litigating position." 488 U.S. 204, 213 (1988). Unlike in *Auer v. Robbins*, 519 U.S. 452, 461-63 (1997), and *Geier v. American Honda Motor Co.*, 120 S. Ct. 1913, 1926-27 (2000), the high-water marks of deference to litigating positions, here the agency's own conduct is at issue and the proposed interpretation of section 154.60 was offered not only in defense of that conduct, but also for the first time in this case. Under such circumstances, the record must contain some evidence that the proposed interpretation reflects the agency's fair and considered judgment. Otherwise, the interpretation represents nothing more than a "*post-hoc* rationalization advanced . . . to defend past agency action against attack." *Auer*, 519 U.S. at 462.

To support its proposed interpretation of section 154.60, the government's brief cites only the affidavit of the very Department of Defense official whose conduct Bigelow challenges. The record, moreover, contains no evidence either of longstanding agency practice consistent with the government's interpretation of section 154.60 or of implicit agency reliance upon that interpretation, nor did Department of Defense attorneys sign the appellate brief. See *Bigelow*, 217 F.3d at 881. Although the government has now informed us that an Air Force lawyer's name appears as *of counsel* on the motion to dismiss in the district court, *see* Opposition to Appellant's Petition for Panel Rehearing and for Rehearing

En Banc at 4, that is hardly sufficient to transform an interpretation of a regulation advanced for the first time as a defensive litigating position into a considered agency judgment worthy of deference.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

STEVEN D.C. BIGELOW
Plaintiff

v. Civil Action No. 98-535

DEPARTMENT OF DEFENSE.
Defendant FILED: JUN 11, 1999

JUDGMENT FOR DEFENDANT

This cause having been considered by the Court on defendants motion for summary judgment, before the Honorable Thomas Penfield Jackson, Judge presiding, and the issues having been duly briefed by all parties and the court having rendered its decision granting defendants motion, now therefore, pursuant to the decision of the Court,

IT IS ORDERED, ADJUDGED AND DECREED that the plaintiff STEVEN D.C. BIGELOW. take nothing on the complaint against the defendant DEPARTMENT OF DEFENSE have and recover costs from the said plaintiff.

NANCY MAYER-WHITTINGTON,
Clerk

Dated: 6-11-99 By: /s/
Robert E. West, Deputy Clerk

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

STEVEN D.C. BIGELOW,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action
No.	)	98-0535 (TPJ)
DEPARTMENT OF DEFENSE,	)	
	)	FILED
Defendant.	)	JUN 11, 1999

ORDER

In accordance with the proceedings at the May 13, 1999 hearing, upon consideration of defendant's motion to dismiss or,in the alternative, for summary judgment, and the entire record herein, it is this 11th day of June, 1999,

ORDERED, that defendant's motion for summary judgment is granted, and it is

FURTHER ORDERED, that the Clerk of Court is directed to enter judgment in favor of defendant Department of Defense and against plaintiff Major Steven D.C. Bigelow, and it is

FURTHER ORDERED, that all pending motions are denied as moot.

/s/
Thomas Penfield Jackson
U.S. District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE THOMAS P. JACKSON

[June 11, 1999]

* * *

Mary Price and David Sheldon for the plaintiff.

Mark Nebeker for the defendants.

Mr. Nebeker: also at counsel table with me is Mr. Barry Walters. (Phonetics.)

The Court: All right. Let me ask you a question, Mr. Nebeker. I have read the papers in the case. I take it that Colonel Noyes was in the direct chain of command; is that correct?

Mr. Nebeker: That's correct, your honor. In fact, the complaint specifically says he was a supervisor to the plaintiff.

The Court: Let me hear from Ms. Price first, if you will.

Ms. Price, I cannot understand how anybody would be more in necessity of knowing pertinent background information about a military officer than his commanding officer.

Ms. Price: But he wasn't his commanding officer. He was his supervisor, your honor.

The Court: Well, all right.

Ms. Price: And there are only particular people who are given access to this information. Commanding officers are given access to the information in order to assess the person's eligibility for access to information in the particular command.

Supervisors are not, your honor. And paragraph 10-100 of the regulation is very clear about that. It doesn't say supervisors cannot, but it lays out very specifically who can, and the people who can are those who provide access—who provide the permission for access.

Paragraph 7-102 says those are commanders.

* * *

Ms. Price: Supervisors, your honor—it's clear from the regulations in paragraph 9-100 that supervisors do have a role in the process. They have a role in the assessment process for an individual. However, what the supervisors' role is, is when they receive adverse information, under paragraph 2-402 of the regulation, what they are to do is to refer that information directly to the defense investigative service, which then makes the decision whether or not it's going to conduct an investigation and determine whether or not the allegations are founded or unfounded.

Paragraph 10-100, your honor, states that personnel security investigative reports may be used only for the purpose of determining eligibility of DOD military personnel, and other persons affiliated, for access to classified information, assignment or retention.

Paragraph 7-102 states that access to classified information shall be granted to persons whose official duties require such access.

It is not an adjudicative function. In other words, it's not the clearance so much, your honor, but rather those are decisions that are made by the commander that acts, as is officially required—not the supervisor.

The Court: Well, who would be making an assignment to your client which would require his access to classified information?

Ms. Price: The commander at the Joint Staff was responsible—

The Court: Then what was Noyes' function?

Ms. Price: Noyes was his supervisor in the office in which he was operating, the Information Warfare and Special Technical Operations. I don't think he was the chief of that office, because he was not the person ultimately who suspended my client's access and had him removed from the Joint Staff office.

In fact, what's interesting about this, your honor, is that initially apparently Colonel Noyes attempted to do the right thing. He made a referral to, I think, the Air Force Office of Special Investigations. They declined to investigate the allegations of misconduct. And that's when he took matters into his own hands and he went to the Joint Staff office, and according to some procedure, which we don't know about and we had asked for discovery on, he was able to gain access to the file.

What else is interesting is whose declaration we don't have is the declaration of Joint Staff Security Officer, who provided him access in the first place, because that is really the missing link in this case—that individual—because it is that individual who, we contend, did not have a basis for believing that his action was grounded in law—that he had a lawful basis for providing this information to a mere supervisor.

Otherwise, access would be available to anybody. I mean anybody in the chain would have access to very, very personal information. And the Privacy Act and these regulations are very comprehensive protections about very, very personal information.

This is information that, you know, a person provides because they are entrusted with very important secrets. As a consequence of being entrusted with those secrets, they have to give up some pretty important secrets themselves. And that information should not be available to anybody. And paragraph 10-100 again makes that point very, very clearly.

"In recognition of the sensitivity of personnel security reports, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion."

And it says further on at paragraph 10-101, "the heads of DOD Components and the Deputy Under Secretary of Defense shall establish the internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports."

We would like discovery to find out what those internal controls are, because we suspect, and we

suggest, and we submit that those internal controls do not provide access to supervisors at Colonel Noyes' level.

Colonel Noyes also referenced in his affidavit a procedure that he followed, but we have been unable to determine what that procedure is. And we would also need discovery to determine that information.

The Court: All right. What do you make of paragraph 9-100 of the directive, which provides this program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process?"

Ms. Price: That paragraph is very important. It doesn't give carte blanche to people to go into investigative reports. What it does do is require of everybody that they be a part of the assessment process.

Part of the assessment process is when you receive adverse information about an individual, who is entrusted with our nation's secrets, you have to do something with that.

You have to read the entire regulation together. Paragraph 2-402 requires that when adverse information is received, it's not investigated. It is referred immediately to the defense investigative service. And that is the agency that has the personnel who are qualified to figure out is this information that makes a difference. They do the investigation.

The Court: I am not sure that they are. Why wouldn't the supervisor be in the best position of all to

determine whether or not an individual represented a security risk? The investigative service is skilled in conducting investigations, not necessarily in assessing the consequences of access to classified information.

Ms. Price: I am sorry, your honor. You're correct about that. What they do do is they produce reports that have been evaluated initially by the central adjudication facility, which is the agency, or the organization, or the component that provides clearance in the first place, and those reports, for the purpose of access, are provided to the commander or to the command.

That is under paragraph 7-102.

The Court: you say Noyes was not the commander. Who was the commander? How far up the chain was the person you identify as the commanding officer?

Ms. Price: The commander would be the person who is in charge of the office in which he was involved, which was the program security office—I am sorry—the Special Operations Office of the Joint Staff. I'm sorry.

We could, of course, use discovery as well on who had access to the report and who was making decisions on that report.

The Court: All right. Let me bear from Mr. Nebeker.

Ms. Price: Thank you, your honor.

The Court: I think your client wants to talk to you.

Mr. Sheldon: I'm sorry. My name is David Sheldon, your honor. I represent Steven Bigelow, who has been promoted to lieutenant colonel very recently by an act of the Secretary of the Air Force. I don't think our position was made.

The Court: Well, who is Ms. Price then? I thought she represented Mr. Bigelow.

Mr. Sheldon: She does as well, your honor. I just wanted to clarify for your honor that a commanding officer in any particular unit makes a decision on whether a person has access to classified information. The individual—the particular individual—and the way the regulations work is that a person has to apply to the government to get a security clearance at any particular level.

The Court: Your client already had a security clearance. The question was whether or not he should be allowed to avail himself of it.

Mr. Sheldon: That's correct, your honor. And in making that determination, a commanding officer cannot access these security reports. He can take an independent action and remove the person, based upon whatever he believes is justified. He can do that, but what he can't do and what—there is a cloak around this information that is very, very sensitive information that is investigated, and then later, a group called the Central Adjudication Facility—and each of the services has one of these—they make a determination about whether the person has a security clearance at any particular level.

At that point, once the person is cleared up, he doesn't automatically have a right to get that informa-

tion. He may have a top secret clearance. Until his commanding officer says, "I give you the ability to see this; you have a need to know this information"—then that's when he gets the information.

And Colonel Noyes had one thing that he could have done—actually two things. He could have, when he learned whatever information he learned—he could have turned over to the Defense Investigative Service or the Joint Staff Security Office—he could have said, "I just found this information out, sir, and I want you to investigate this. I want to make sure he doesn't have—that he is all right—that he is not a security risk." But what can[*] happen is the Joint Staff Security Officer to turn over information to Colonel Noyes and say, "this is some other information that we found out." And that's exactly what happened in this case, your honor.

So, your honor's question is very, very important in terms of what a supervisor can or can't do. And I understand that it's a logical assumption that the C.E.O.—the skipper of a ship has an obligation to assess and everything. That is what the regulation says. That's the specific paragraph that you said where the supervisor provides information and cooperates with the assessor.

That is true. He cooperates with the J.S.S.O., the Joint Staff Security Office, or with the Defense Investigative Service, or whoever it is, but what he doesn't get is the cloak of information behind there.

---

[*] *Sic*; should read "cannot" (footnote added).

It is an one-way flow of information. It's not two ways, and the reason that that's so is because we don't want supervisors—the military doesn't want supervisors having access to this very, very personal information. And that is universal within the regulation. And the reason is because these supervisors have to assess a person as far as their duty performance. They don't need to know that they have X, Y and Z.

The government has set up a separate compartment, the Central Adjudication Facility, to make that assessment on whether the person is entitled to a security clearance.

The Court: All right.

Mr. Sheldon: I apologize, your honor.

The Court: All right, Mr. Nebeker.

Mr. Nebeker: I just have to take issue with that, your honor. I look at 9-100. First of all, it talks about the supervisor is included within the people that are supposed to exchange information. It says that there is a continuing responsibility to—a continuing assessment has to be done of whether somebody should have access to this classified type of information.

So it's not just that, okay, he now has security clearance that's been given to him by this one component, but that has to be ongoing. The whole purpose is so that the military doesn't—you don't have a supervisor saying, "hey, I know I found this derogatory information, but it's not my job to go find out whether he should still have access to this classified information." That is exactly what the regulation is designed to

prohibit.

Let me just point out a couple of other things, your honor. The plaintiff, through counsel, has now argued that he didn't have any role, once he passed that information over.

The language from 9-100 says the information should be shared. And there are a couple of other parts of this DOD regulation that talk about how these standards should be applied, based on all available information.

That's found in paragraph 2-101, and I think also in 2-200. In paragraph 2-306, it talks about Special Investigative Inquiries. That is what apparently plaintiff alleges and I guess our declaration supports. Colonel Noyes referred this matter for Special Investigative Inquiry. Interestingly enough, under 2-306(c), if the requester of an investigative inquiry isn't satisfied, he can then forward on to the Deputy Under-Secretary of Defense for Policy his disagreement and get a higher level of review of whether or not they are going to investigate or what they are going to investigate. In order to make that type of a determination, he, of course, has to know whether this is the kind of thing he wants to fight about, and the only way he can get that is to fulfill his responsibility as the supervisor and see what information they have.

If they know that—I am just going to pick a hypothetical here—that Mr. Bigelow was lost near enemy lines in wartime or something, and they couldn't figure out where he was, and they are trying to figure out if he is, maybe, meeting with a spy—well, the fact that he is missing once, it might be relevant to know

whether they want to seek higher-level approval or higher-level review of the decision not to investigate a subsequent unexplained absence to find out if he had ever done it before.

There is nothing wrong with that. And that, of course, dovetails with the Privacy Act, which says that records are able to be reviewed by employees within the agency who have a duty to access the records in the course of their employment. That's exactly what this supervisor was doing here.

There are a couple of other things that argue against the idea that once you pass off the information, you're done—the fact that under paragraph 8-102, there is a mechanism whereby you can suspend an individual or suspend their access to classified information.

That deals with the assignment. That doesn't deal with whether they have a clearance. That just deals with whether they are going to get the information. And if you're waiting in the interim for a special investigative inquiry to be conducted to determine whether or not further inquiry is going to be made, that's the kind of thing that a supervisor has to decide. "Am I going to let him into that office today to look over that classified information?"

So I would argue to the court that based upon the regulation itself, and the fact that the plaintiff has admitted in the complaint that Noyes was the supervisor, that the plaintiff had access to the nation's most sensitive secrets, and that Noyes learned of allegations of misconduct that caused this whole thing to start up, it seems like there is no—it seems to me there is no doubt that they have failed to state a claim because, in

essence, they shoot themselves in the foot when they say he is a supervisor. And we know from the regs that the supervisor has this ongoing responsibility.

The Court: Well, I wish the regs were a little more explicit. It is rather turgid regulation writing.

Mr. Nebeker: I understand, your honor.

The Court: But intuitively, based upon, among other things, my own personal military experience, I know that if derogatory information had come to the attention of my commanding officer, he would have said, "Lieutenant, look into this and see whether or not there is a basis to take seamen so and so off of assignment."

Mr. Nebeker: Right. And that's exactly—

The Court: It is so fundamental that I am assuming that the regulation must say that.

Mr. Nebeker: Well, in fact, 9-100 does say that.

Now, also, I will point out, plaintiffs were talking about discovery. They want to know what the procedures are.

I asked if there were other written procedures on how this is accomplished, and I found that there were none. I would have filed them with the court. Maybe they would have clarified for the court this rather lengthy regulation, but the bottom line is the common-sense approach. They say throughout the regulation that it should be fulfilled using common sense, but also with access to all available information. And it only makes sense.

Finally, the plaintiffs suggested that they needed discovery in various areas. I would point out to the court that we're referring to the regulation, and I think, to that extent, it's the law. It's written down. It's not in dispute. But if the court were inclined to go beyond it and include the declaration that Colonel Noyes included—of recent, the Court of Appeals has come down with a couple of cases that suggest that the court has discretion to grant summary judgment, even prediscovery. This would be a perfect case for it. Those cases include the Joann Carpenter case versus Federal National Mortgage Association, 98-7170, from April of '99—April 27th of '99 at page 8 of the slip opinion. And the other one is Daniel M. Byrd, III, versus E.P.A., 98-5180—

The Court: I don't think discovery is necessary in the case.

Mr. Nebeker: I would have to agree. I don't think the court abused its discretion in any way, shape or form. When you look at the regulation and the allegations in the complaint, it seems pretty clear to me that this is exactly the kind of circumstance that the Department of Defense intends a supervisor to investigate—not to go out and interview witnesses and so forth, but to gather the information available within the command. And that's exactly what was done here. And we would submit that in light of that, our motion to dismiss or for summary judgment should be granted, your honor.

The Court: All right. I am going to grant the motion. I suggest that you take it to the Court of Appeals, and if I have misapprehended the import of the regulations, they will let me know. They have shown no

reluctance in the past to let me know.

Ms. Price: Thank you, your honor.

The Court: So I am sure that we'll find out.

PRIVACY ACT OF 1974
[Excerpts]

§ 552a. Records maintained on individuals

(a) Definitions.—For purposes of this section—

(1) the term "agency" means agency as defined in section 552(e) of this title;

(2) the term "individual" means a citizen of the United States or alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

* * *

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

* * *

(13) the term "Federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) Conditions of disclosure.—No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

* * *

(c) Accounting of certain disclosures.—Each agency, with respect to each system of records under its control, shall—

(1) except for disclosure made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of—

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) Access to records.—Each agency that maintains a system of records shall—

(1) upon request by any individual to gain access to his record or to any information per-

taining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and—

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either—

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency,

and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such a refusal, and not later that 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual request such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the records in accordance with the request, permit the individual to file with the agency a concise statement setting forth reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provided copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in

reasonable anticipation of a civil action or proceeding.

(e) Agency requirements.—Each agency that maintains a system of records shall—

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include—

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the

First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirement of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data,

views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) Agency rules.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the am-

endment of any record or information pertaining to the individual, for making a determination, on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)(1) Civil remedies.—Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) falls to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be

made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the

agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be

brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) Rights of legal guardians.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) Criminal penalties.—Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more then $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

(j) General exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)-(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is-

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under

section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) Specific exemptions.—The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is—

(1) subject to the provisions of section 552(b)(1) of this title,

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to

section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military, service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

* * *

(t)(1) Effect of other laws.—No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

* * *

DEPARTMENT OF DEFENSE
PERSONNEL SECURITY PROGRAM
32 C.F.R. Pt. 154
[Excerpts]

§ 154.2 Applicability.

* * *

(b) All provisions of this part apply to DoD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, contractor personnel and other personnel who are affiliated with the Department of Defense except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22-R and in 32 CFR part 155.

* * *

§ 154.3 Definitions.

(a) *Access*. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

(b) *Adverse action*. A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

(c) *Background Investigation (BI).* A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph 3, Appendix A, this part, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

(d) *Classified information.* Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356.

(e) *Defense Clearance and Investigative Index (DCII).* The DCII is the single, automated, central DoD repository which identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities.

(f) *DoD component.* Includes the Office of the Secretary of Defense; the Military Departments; Chairman of the Joint Chiefs of Staff; Directors of Defense Agencies and the Unified and Specified Commands.

(g) *Entrance National Agency Check (ENTNAC).* A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

(h) *Head of DoD component.* The Secretary of Defense; the Secretaries of the Military Departments; the Chairman of Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands; and the

Directors of Defense Agencies.

(i) *Immigrant alien*. Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

(j) *Interim security clearance*. A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

(k) *Limited access authorization*. Authorization for access to Confidential or Secret information granted to non-US. citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (paragraph 3, Appendix A).

(l) *Minor derogatory information*. Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

(m) *National Agency check (NAC)*. A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, Appendix A, this part, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

(n) *National Agency Check Plus Written Inquiries (NACI)*. A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies,

former employers and supervisors, references and schools.

(o) *National security.* National security means the national defense and foreign relations of the United States.

(p) *Need-to-know.* A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official U.S. Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

(q) *Periodic Reinvestigation (PR).* An investigation conducted every five years for the purpose of updating a previously completed background investigation, special background investigation, single scope background investigation or PR on persons occupying positions referred to in § 154.19. Investigative requirements are as prescribed in appendix A to part 154, section 5. The period of investigation will not normally exceed the most recent 5-year period.

(r) *Personnel Security Investigation (PSI).* Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investi-

gation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see § 154.9(d)) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

(s) *Scope*. The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

(t) *Security clearance*. A determination that a person is eligible under the standards of this part for access to classified information.

(u) *Senior Officer of the Intelligence Community (SOIC)*. The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

(v) *Sensitive position*. Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in § 154.13(b).

(w) *Significant derogatory information*. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

(x) *Special access program*. Any program imposing need-to-know or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need-to-know.

(y) *Special Background Investigation (SBI)*. A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph 4, Appendix B, this part. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

(z) *Special Investigative Inquiry (SII)*. A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provisions of this part.

(aa) *Service*. Honorable active duty (including attendance at the military academies), membership in

ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DoD contractor or as a consultant involving access under the DoD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

(bb) *Unfavorable administrative action*. Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this part.

(cc) *Unfavorable personnel security determination*. A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this part; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

(dd) *United States Citizen (Native Born)*. A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the United States).

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61024, Nov. 19, 1993]

* * *

§ 154.9 Authorized personnel security investigative agencies.

(a) *General.* The DIS provides a single centrally directed personnel security investigative service to conduct personnel security investigations within the 50 States, District of Columbia, and Commonwealth of Puerto Rico for DoD Components, except as provided for in DoD Directive 5100.23 [1]. DIS will request the Military Departments or other appropriate Federal Agencies to accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Under Secretary of Defense for Policy. In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

(b) *Subversive affiliations*—(1) *General.* In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

(i) Overthrowing the Government of the United States or the government of a State;

---

[1] See footnote 1 to § 154.2(c). [Footnote in original.]

(ii) Substantially impairing for the purpose of influencing U.S. Government policies or decisions: (A) The functions of the Government of the United States, or (B) The functions of the government of a State;

(iii) Depriving persons of their civil rights under the Constitution or laws of the United States.

(2) *Military Department/FBI jurisdiction*. Allegations of activities covered by § 154.7 (a) through (f) are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI. Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a personnel security investigation conducted by DIS, they shall be referred immediately to either the FBI or to a military department counterintelligence agency, as appropriate.

(3) *DIS jurisdiction*. Allegations of activities limited to those set forth in § 154.7 (g) through (j) of this part shall be investigated by DIS.

(c) *Suitability information*—(1) *General*. Most derogatory information developed through personnel security investigations of DoD military or civilian personnel is so-called suitability information, that is, information pertaining to activities or situations covered by § 154.7 (g) through (q). Almost all unfavorable personnel security determinations made by DoD authorities are based on derogatory suitability information, although such information is often used as a basis for

unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal from Federal employment under OPM regulations.

(2) *Pre-clearance investigation*. Derogatory suitability information, except that covered in paragraph (c)(4) of this section, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to § 154.7 (g) through (q).

(3) *Postadjudication investigation*. Derogatory suitability allegations, except those covered by paragraph (c)(4) of this section arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a Special Investigative Inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when § 154.19(b) applies. Postadjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations lie outside the DoD personnel security program and are not a

proper investigative function for departmental counterintelligence organizations, Component personnel security authorities, or DIS.

(4) *Allegations of criminal activity*. Any allegations of conduct of a nature indicating possible criminal conduct, including any arising during the course of a personnel security investigation, shall be referred to the appropriate DoD, military department or civilian criminal investigative agency. Military department investigative agencies have primary investigative jurisdiction in cases where there is probable cause to believe that the alleged conduct will be the basis for prosecution under the Uniform Code of Military Justice.

(d) *Hostage situations*—(1) *General*. A hostage situation exists when a member of an individual's immediate family or such other person to whom the individual is bound by obligation or affection resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this category of investigation is based on the possibility that an individual in such a situation might be coerced, influenced, or pressured to act contrary to the best interests of national security.

(2) *DIS jurisdiction*. In the absence of evidence of any coercion, influence or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by DIS.

(3) *Military Department and/or FBI jurisdiction*. Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned—or should there exist any other

evidence that the individual is actually being coerced, influenced, or pressured by an element inimical to the interests of national security—then the case becomes a counterintelligence matter (outside of investigative jurisdiction of DIS) to be referred to the appropriate military department or the FBI for investigation.

(e) *Overseas personnel security investigations.* Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate military department investigative organization. Only postadjudication investigations involving an overseas subject may be referred by the requester directly to the military department investigative organization having investigative responsibility in the overseas area concerned (see Appendix I) with a copy of the investigative request sent to DIS. In such cases, the military department investigative agency will complete the investigation, forward the completed report of investigation directly to DIS, with a copy to the requester.

* * *

Subpart G—Issuing Clearance and Granting Access

§ 154.47 General.

(a) The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the

individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of § 154.56(b).

(b) Only the authorities designated in paragraph A, Appendix E are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in § 154.55(b) of this part are complied.

(c) All commanders and heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this part.

Subpart H—Unfavorable Administrative Actions

§ 154.55 Requirements.

(a) *General*. For purposes of this part, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at § 154.3 and any unfavorable personnel security determination, as defined at § 154.3. This subpart is intended only to provide guidance for the

internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

(b) *Referral for action.* (1) Whenever derogatory information relating to the criteria and policy set forth in § 154.7(a) and Appendix H of this part is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall insure that the parent Component of the individual concerned is informed promptly concerning the derogatory information developed and any actions taken or anticipated with respect thereto. However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with § 154.56(b), if such action is warranted and supportable by the criteria and policy contained in § 154.7(a) and Appendix H. No unfavorable administrative action as defined in § 154.3 may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in § 154.56(b) or, in the case of SCI, Annex B, DCID 1/14.

(2) The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General "hotline" to receive such reports for appropriate follow-up by DIS. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

(c) *Suspension.*

(1) The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subject's security status unchanged or to take interim action to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability to intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the appropriate authority designated in appendix F to this part.

(2) Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), the individual concerned must be notified of the determination in writing by the commander, or head of the component or

adjudicative authority, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

(3) Component field elements must promptly report all suspension actions to the appropriate central adjudicative authority, but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the DCII Eligibility and Access fields to alert all users to the individual's changed status.

(4) Every effect[*] shall be made to resolve suspension cases as expeditiously as circumstances permit. Suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be reported to the DASD(CI&SCM) for review and appropriate action.

(5) A final security clearance eligibility determination shall be made for all suspension actions and the determination entered in the DCII. If, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the "Z" Code (adjudication action incomplete due to loss of jurisdiction) if the clearance eligibility field is appropriate. In no case shall a "suspension" code (Code Y) remain as a permanent record in the DCII.

(6) A clearance or access entry in the DCII shall not be suspended or downgraded based solely on the fact

---

[*] *Sic*; should read "effort" (footnote added).

that a periodic reinvestigation was not conducted precisely within the 5 year time period for TOP SECRET/SCI or within the period prevailing for SECRET clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed time frame, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

(d) *Final unfavorable administrative actions.* The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in Appendix E, except that the authority to terminate the employment of a civilian employee of a military department or Defense agency is vested solely in the head of the DoD component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DoD Components, on the basis of criteria listed in § 154.7 (a) through (f), shall be coordinated with the Deputy Under Secretary of Defense for Policy prior to final action by the head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this part if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the military departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the central adjudication facility to continue for process the individual for denial or revocation of a security clearance, access to classified information on or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this part.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§ 154.56 Procedures.

(a) *General.* No final personnel security determination shall be made on a member of the Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in paragraph (b) of this section when such determination results in an unfavorable administrative action (see § 154.55(a)). As an exception, Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by 32 CFR part 253.

(b) *Unfavorable administrative action procedures.* Except as provided for below, no unfavorable administrative action shall be taken under the authority of this part unless the person concerned has been given:

(1) A written statement of the reasons why the unfavorable administrative action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of the Privacy Act of 1974 (5 U.S.C. 552a) and national security permit. The statement will also provide the name and address of the agencies (agencies) to which the individual may write to obtain a copy of the investigative file(s) upon which the unfavorable administrative action is being taken. Prior to issuing a statement of reasons to a civilian employee for suspension or removal action, the issuing authority must comply with the provisions of Federal Personnel Manual, chapter 732, subchapter 1, paragraph 1-6b. The signature authority

must be as provided for in § 154.41(b) (1)(ii) and (2)(ii).

(2) An opportunity to reply in writing to such authority as the head of the Component concerned may designate;

(3) A written response to any submission under subparagraph b. stating the final reasons therefor, which shall be as specific as privacy and national security considerations permit. The signature authority must be as provided for in § 154.41(b) (1)(ii) and (2)(ii). Such response shall be as prompt as individual circumstances permit, not to exceed 60 days from the date of receipt of the appeal submitted under paragraph (b)(2) of this section provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the subject must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not, in any case, exceed a total of 90 days from the date of receipt of the appeal under paragraph (b) of this section.

(4) An opportunity to appeal to a higher level of authority designated by the Component concerned.

(c) *Exceptions to policy*. Notwithstanding paragraph (b) of this section or any other provision of this part, nothing in this part shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to section 7532, title 5, U.S. Code. Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph (b)

of this section are not appropriate. Such determination shall be conclusive.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

* * *

Subpart I—Continuing Security Responsibilities

§ 154.60 Evaluating continued security eligibility.

(a) *General.* A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to assure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process.

(b) *Management responsibility*. (1) Commanders and heads of organizations shall insure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this part) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

(2) The heads of all DoD components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long term, job-related security problems.

(c) *Supervisory responsibility*. Security programs shall be established to insure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individual's continued eligibility for access.

(1) In conjunction with the submission of PRs stated in § 154.19, and paragraph 5, Appendix A, super-

visors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's continued eligibility for access to classified information is omitted.

(2) If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package:

I am aware of no information of the type contained at Appendix D, 32 CFR part 154, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information.

(3) If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

I am aware of information of the type contained in Appendix D, 32 CFR part 154, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s).

(4) In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accor-

dance with paragraphs (c) (2) and (3) of this section as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

(d) *Individual responsibility.* (1) Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

(2) Moreover, individuals having access to classified information must report promptly to their security office:

(i) Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

(A) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(B) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

(ii) Any information of the type referred to in § 154.7 or appendix H to this part.

(e) *Co-worker responsibility.* Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

* * *

Subpart J—Safeguarding Personnel Security Investigative Records

§ 154.65 General.

In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DoD military and civilian personnel, contractor employees, and other persons affiliated with the Department of Defense, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counterintelligence investigations. Other uses are subject to the specific written authorization of the Deputy Under Secretary of Defense for Policy.

§ 154.66 Responsibilities.

DoD authorities responsible for administering the DoD personnel security program and all DoD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this part and that such reports and records are safeguarded as prescribed herein. The heads of DoD Components and the Deputy Under Secretary of Defense for Policy for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by §§ 154.67 and 154.68.

§ 154.67 Access restrictions.

Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with 32 CFR parts 286 and 286a and with the following:

(a) DoD personnel security investigative reports shall be released outside of the DoD only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

(b) Within DoD, access to personnel security investigative reports shall be limited to those designated DoD officials who require access in connection with specifically assigned personnel security duties, or other activities specifically identified under the provisions of § 154.65.

(c) Access by subjects of personnel security investigative reports shall be afforded in accordance with

32 CFR part 286a.

(d) Access to personnel security clearance determination information shall be made available, other than provided for in paragraph (c) of this section, through security channels, only to DoD or other officials of the Federal Government who have an official need for such information.

§ 154.68 Safeguarding procedures.

Personnel security investigative reports and personnel security determination information shall be safeguarded as follows:

(a) Authorized requesters shall control and maintain accountability of all reports of investigation received.

(b) Reproduction, in whole or in part, of personnel security investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

(c) Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lockbar and an approved three-position dial-type combination padlock or in a similarly protected area/container.

(d) Reports of DoD personnel security investigations shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows:

TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATION

(e) An individual's status with respect to a personnel security clearance or a Special Access authorization is to be protected as provided for in 32 CFR part 286.

§ 154.69 Records disposition.

(a) Personnel security investigative reports, to include OPM NACIs may be retained by DoD recipient organizations, only for the period necessary to complete the purpose for which it was originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with 32 CFR part 159.

(b) DoD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor derogatory nature 15 years after the date of the last action. That is, after the completion date of the investigation or the date on which the record was last released to an authorized user—whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of a significant nature due to information contained in the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and

those of widespread public or congressional interest may be offered to the National Archives after 15 years.

(c) Personnel security investigative reports on persons who are considered for affiliation with DoD will be destroyed after 1 year if the affiliation is not completed.

DEPARTMENT OF DEFENSE
PRIVACY PROGRAM
32 C.F.R. Pt. 310
[Excerpt]

Subpart E—Disclosure of Personal Information to Other Agencies and Third Parties

§ 310.41 Nonconsensual disclosures.

(a) *Disclosures within the Department of Defense.* (1) Records pertaining to an individual may be disclosed without the consent of the individual to any DoD official who has need for the record in the performance of his or her assigned duties.

(2) Rank, position, or title alone do not authorize access to personal information about others. An official need for the information must exist before disclosure.

* * *

THE JOINT STAFF
WASHINGTON, DC

19 August 1997

IMD-97-00009

David P. Sheldon
Feldesman, Tucker, Leifer, Fidell & Bank
Attorneys at Law
2001 L Street, NW Third Floor
Washington, DC 20036-4910

Dear Mr. Sheldon:

This is in response to your request of 10 July 1997 asking for an accounting of disclosures of Major Bigelow's prior background investigations while under the Joint Staff's control.

This request is redundant in that it duplicates one made by Major Bigelow on 31 January 1997 and responded to by my office, the information Management Division, Joint Secretariat, on 13 February 1997. A review of that response finds that it is complete and accurate.

The only disclosures made by the Joint Staff regarding Major Bigelow's prior background investigation were made to officers and/or employees of the agency who had a need to know for the performance of their duties. Under Section 552a(c)(1) of the Privacy Act, such disclosures are exempt from accounting requirements. The disclosure to Colonel Noyes of the Joint Staff falls within this exemption.

Sincerely,

/s/
Edmund F. McBride
Chief, Information Management Division
Secretariat, Joint Staff

DECLARATION OF COLONEL NATHAN W. NOYES

(1) I am currently the Commander of the 21st Cavalry Brigade, Fort Hood, Texas. I was formerly the Chief, Information Warfare and Special Technical Operations Center (IWSTOC), United States National Military Command Center, Joint Chiefs of Staff (JCS), the Pentagon, from June of 1995 through October of 1996. As such, I was the supervisor Major Steven C. Bigelow, U.S. Air Force. All information contained herein is based upon my personal knowledge gained in my official capacity as Chief of the IWSTOC.

(2) All positions within IWSTOC are staffed by personnel possessing the highest levels of security classification, above and beyond TOP SECRET. In fact, even the names of those security classifications are classified. As a supervisor, I was familiar with my responsibilities with regard to ensuring that all personnel within my purview maintained the highest standards of personal and professional conduct such that extremely sensitive national security information would not be compromised. In the event that I believed that any of my personnel failed to meet these standards, I was responsible for deciding whether or not such conduct impacted on their ability to be entrusted with the nation's most closely guarded military secrets.

(3) Sometime in the Fall of 1995, I became aware of instances of personal and professional misconduct on the part of Major Bigelow which caused me to question his character and integrity. Some of these instances can not be related without disclosing classified information, but the following is a brief outline of some of the unclassified instances of misconduct with which I became familiar.

(4) Major Bigelow was believed to have committed travel voucher fraud with regards to his whereabouts while on leave in conjunction with official travel, and he was shown by the Air Force to have failed to account for several periods of paid leave. Additionally, Major Bigelow was believed to have utilized his government computer for illicit and improper purposes. Finally, and of utmost importance, Major Bigelow sometimes disappeared in foreign countries near sensitive international borders. In short, Major Bigelow's personal conduct and lifestyle appeared to be inconsistent with his duties and responsibilities as a member of IWSTOC, and caused me, as his supervisor, to question his character, trustworthiness, and integrity.

(5) Consequently, I went to the Joint Staff Security Office and requested Major Bigelow's personnel security file because it was my considered opinion that he was lying abut certain aspects of his past. The procedure is such that a personnel security specialist will access the file and then review it with the supervisor, provided that the supervisor has the appropriate clearance level, which I did. My review confirmed my belief that Major Bigelow had misrepresented certain aspects of his past, and I referred the matter to the Air Force for disciplinary action. As a result, Major Bigelow was relieved of his duties at IWSTOC.

(6) As Chief of the Information Warfare and Special Technical Operations Center, I had an official need to know the information in the personnel security file of any employee under my supervision in order to protect the interests of national security; particularly where I was investigating allegations of misconduct.

* * *

AFFIDAVIT OF STEVEN D. C. BIGELOW IN SUPPORT OF PLAINTIFF'S MOTION TO CONDUCT LIMITED DISCOVERY

* * *

1. I am the plaintiff in the above-captioned action. I make this statement in accordance with Rule 56(f) of the Federal Rules of Civil Procedure, and in support of my request for an opportunity to conduct limited discovery before being required to respond to Defendant's Motion to Dismiss, or, in the Alternative, for Summary Judgment.

2. As explained in the motion to which this affidavit is attached, defendant's declarant Colonel Nathan W. Noyes, and other, as yet unknown, employees of the Department of Defense, have knowledge regarding the procedure declarant followed to gain access to my security file. In contrast, and despite my efforts through counsel, I lack such knowledge. The only way for me to obtain this knowledge is by allowing my attorneys to engage in limited discovery, by taking the depositions of Colonel Noyes and other, as yet unknown, employees of defendant, serve them interrogatories, and/or seek the production of documents.

3. As explained in the motion to which this affidavit is attached, defendant's declarant Colonel Noyes, has knowledge of information contained in my security file that declarant examined and which led to my subsequent reassignment. In contrast, and despite my efforts to through counsel, I lack such knowledge. The only way I can be expected to obtain this knowledge is by allowing my attorneys to take his deposition, serve him interrogatories, and/or seek the production of docu-

ments.

4. As explained in the motion to which this affidavit is attached, defendant's declarant, Colonel Noyes and other, as yet unknown, members of the Central Adjudication Facility, have knowledge pertaining to my initial security clearance and how declarant's review of such information led to my subsequent reassignment. In contrast, and despite my efforts through counsel, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take their depositions, serve them interrogatories and/or seek the production of documents.

5. As explained in the motion to which this affidavit is attached, defendant's declarant, Colonel Noyes and other, as yet unknown, members of the Defense Investigative Service, have knowledge pertaining to a security investigation of me conducted in 1993 and how declarant's subsequent review of my security file led to my reassignment. In contrast, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take their depositions, serve them interrogatories and/or seek the production of documents.

6. As explained in the motion to which this affidavit is attached, defendant's declarant, Colonel Noyes and other, as yet unknown, members of the Joint Staff Security Office, including an unnamed security specialist, have information regarding who in that office afforded Colonel Noyes access to my security file and assisted him during the examination, and under what authority they did so. In contrast, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take their

depositions, serve them interrogatories and/or seek the production of documents.

7. As explained in the motion to which this affidavit is attached, as yet unknown employees of the defendant and defendant's Joint Staff Security Office have knowledge regarding whether, and if so, by what authority, the Joint Staff Security Office maintained my security file beyond the 90-day period permitted by Department of Defense regulation 5200.2-R § 10-104(a). In contrast, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take their depositions, serve them interrogatories and/or seek the production of documents.

8. As explained in the motion to which this affidavit is attached, declarant and, as yet unknown employees of Defense Investigative Service have knowledge regarding whether and to what extent that office conducted a, post-adjudicative, Special Investigation Inquiry, and any report and conclusions of the inquiry. In contrast, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take their depositions, serve them interrogatories, and/or seek the production of documents.

9. As explained in the motion to which this affidavit is attached, the as yet unknown officer in charge of the Joint Staff Security Office has knowledge regarding procedures that office follows in assessing post-adjudicative security concerns, and may have knowledge regarding the review of my security file. In contrast, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take that officer's deposition, serve the officer interrogatories, and/or seek the production of documents.

10. As explained in the motion to which this affidavit is attached, the as yet unknown officer with primary responsibility for administering Department of Defense Regulation 5200.2-R has knowledge regarding the procedures followed when assessing post-adjudicative security concerns, and may have knowledge regarding the procedures followed in reviewing my security file. In contrast, I lack such knowledge. The only way I can be expected to obtain such knowledge is by allowing my attorneys to take that officer's deposition, serve the officer interrogatories, and/or seek the production of documents.

* * *